



Gestione el acceso a archivos mediante SMB

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap/smb-admin/local-users-groups-concepts-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione el acceso a archivos mediante SMB	1
Utilice usuarios y grupos locales para autenticación y autorización	1
Cómo utiliza ONTAP usuarios y grupos locales	1
Qué privilegios locales son	5
Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores SMB de ONTAP	7
Requisitos para las contraseñas de usuarios locales de ONTAP SMB	7
Grupos BUILTIN predefinidos y privilegios SMB de ONTAP predeterminados	8
Habilite o deshabilite la funcionalidad de grupos y usuarios locales	9
Permite gestionar cuentas de usuario local	12
Administrar grupos locales	16
Gestione los privilegios locales	23
Configurar la comprobación de recorrido de derivación	27
Obtenga información sobre cómo configurar la comprobación de travesía de derivación de SMB de ONTAP	27
Permitir que los usuarios o grupos omitan la verificación del recorrido del directorio SMB de ONTAP ..	29
No permitir que usuarios o grupos omitan la comprobación del recorrido del directorio SMB de ONTAP	30
Muestra información acerca de las políticas de auditoría y seguridad de archivos	31
Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos SMB de ONTAP	31
Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad NTFS	32
Mostrar información sobre la seguridad de los archivos SMB de ONTAP en volúmenes de estilo de seguridad mixto	38
Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad UNIX	41
Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NTFS en volúmenes SMB FlexVol	44
Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes SMB FlexVol	47
Aprenda a mostrar información sobre políticas de auditoría y seguridad de archivos SMB de ONTAP ..	48
Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI	50
Comandos ONTAP para administrar la seguridad de archivos NTFS de SMB, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento	50
Comandos ONTAP para configurar la seguridad de archivos y carpetas SMB	52
Conozca los límites al usar comandos ONTAP para configurar la seguridad de archivos y carpetas SMB	52
Utilice descriptores de seguridad para aplicar la seguridad de archivos y carpetas SMB de ONTAP ...	52
Obtenga información sobre cómo aplicar políticas de directorio de archivos que utilizan usuarios o grupos SMB locales en el destino de recuperación ante desastres de ONTAP SVM	53
Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI	56

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos	64
Obtenga información sobre cómo administrar los trabajos de políticas de seguridad de ONTAP SMB ..	72
Comandos ONTAP para administrar descriptores de seguridad NTFS en servidores SMB	73
Comandos ONTAP para administrar entradas de control de acceso DACL NTFS en servidores SMB ..	73
Comandos ONTAP para administrar entradas de control de acceso SACL NTFS en servidores SMB ..	74
Comandos de ONTAP para administrar políticas de seguridad SMB	74
Comandos ONTAP para administrar tareas de políticas de seguridad SMB	75
Comandos de ONTAP para administrar trabajos de políticas de seguridad de SMB	75
Configure la caché de metadatos para los recursos compartidos de SMB	76
Obtenga más información sobre el almacenamiento en caché de metadatos SMB de ONTAP	76
Habilitar la caché de metadatos SMB de ONTAP	76
Configurar la duración de las entradas de caché de metadatos SMB de ONTAP	77
Administrar bloqueos de archivos	78
Obtenga información sobre el bloqueo de archivos SMB de ONTAP entre protocolos	78
Obtenga información sobre los bits de solo lectura de ONTAP SMB	79
Diferencias entre ONTAP y Windows en el manejo de bloqueos en componentes de ruta de acceso compartida	80
Mostrar información sobre los bloqueos SMB de ONTAP	80
Romper los bloqueos SMB de ONTAP	82
Supervise la actividad del SMB	83
Mostrar información de la sesión SMB de ONTAP	83
Mostrar información sobre archivos SMB de ONTAP abiertos	87
Determinar qué estadísticas, objetos y contadores están disponibles en los servidores SMB de ONTAP	90
Mostrar estadísticas de ONTAP SMB	94

Gestione el acceso a archivos mediante SMB

Utilice usuarios y grupos locales para autenticación y autorización

Cómo utiliza ONTAP usuarios y grupos locales

Obtenga información sobre los usuarios y grupos locales de ONTAP SMB

Debe saber cuáles son los usuarios y grupos locales, así como alguna información básica sobre ellos, antes de determinar si configurar y utilizar usuarios y grupos locales en su entorno.

- **Usuario local**

Una cuenta de usuario con un identificador de seguridad único (SID) que solo tiene visibilidad en la máquina virtual de almacenamiento (SVM) donde se crea. Las cuentas de usuario local tienen un conjunto de atributos, incluidos el nombre de usuario y el SID. Una cuenta de usuario local autentica de forma local en el servidor CIFS mediante la autenticación NTLM.

Las cuentas de usuario tienen varios usos:

- Se utiliza para otorgar privilegios *User Rights Management* a un usuario.
- Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Grupo local**

Un grupo con un SID exclusivo tiene visibilidad solo en la SVM donde se crea. Los grupos contienen un conjunto de miembros. Los miembros pueden ser usuarios locales, usuarios de dominio, grupos de dominio y cuentas de equipos de dominio. Los grupos se pueden crear, modificar o eliminar.

Los grupos tienen varios usos:

- Se utiliza para otorgar privilegios *User Rights Management* a sus miembros.
- Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Dominio local**

Un dominio que tiene un alcance local, delimitado por la SVM. El nombre del dominio local es el nombre del servidor CIFS. Los usuarios y grupos locales se encuentran dentro del dominio local.

- **Identificador de seguridad (SID)**

Un SID es un valor numérico de longitud variable que identifica los principios de seguridad de estilo Windows. Por ejemplo, un SID típico toma la siguiente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticación NTLM**

Un método de seguridad de Microsoft Windows que se utiliza para autenticar usuarios en un servidor

CIFS.

- **Base de datos replicada en cluster (RDB)**

Base de datos replicada con una instancia en cada nodo de un clúster. Los objetos de usuario local y de grupo se almacenan en el RDB.

Razones para crear usuarios y grupos locales de ONTAP SMB

Hay varias razones para crear usuarios locales y grupos locales en la máquina virtual de almacenamiento (SVM). Por ejemplo, puede tener acceso a un servidor SMB utilizando una cuenta de usuario local si los controladores de dominio (DC) no están disponibles, es posible que desee utilizar grupos locales para asignar privilegios o que el servidor SMB esté en un grupo de trabajo.

Es posible crear una o varias cuentas de usuario locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los usuarios del dominio no están disponibles.

Los usuarios locales son necesarios en configuraciones de grupos de trabajo.

- Puede autenticar e iniciar sesión en el servidor SMB si las controladoras de dominio no están disponibles.

Los usuarios locales pueden autenticarse con el servidor SMB mediante la autenticación NTLM cuando el controlador de dominio está inactivo o cuando los problemas de red impiden que el servidor SMB se ponga en contacto con el controlador de dominio.

- Desea asignar privilegios *User Rights Management* a un usuario local.

User Rights Management es la capacidad de un administrador de servidor SMB para controlar los derechos que tienen los usuarios y los grupos en la SVM. Puede asignar privilegios a un usuario asignando los privilegios a la cuenta del usuario o haciendo que el usuario sea miembro de un grupo local que tenga esos privilegios.

Se pueden crear uno o varios grupos locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los grupos de dominio no están disponibles.

Los grupos locales no son necesarios en las configuraciones de grupos de trabajo, pero pueden ser útiles para administrar privilegios de acceso para los usuarios de grupos de trabajo locales.

- Desea controlar el acceso a los recursos de archivos y carpetas mediante grupos locales para controlar el uso compartido y el acceso a archivos.
- Desea crear grupos locales con privilegios *User Rights Management* personalizados.

Algunos grupos de usuarios integrados tienen privilegios predefinidos. Para asignar un conjunto personalizado de privilegios, puede crear un grupo local y asignar los privilegios necesarios a ese grupo. A continuación, puede agregar usuarios locales, usuarios de dominio y grupos de dominio al grupo local.

Información relacionada

- [Obtenga más información sobre la autenticación de usuarios locales](#)
- [Lista de privilegios compatibles](#)

Obtenga información sobre la autenticación de usuarios SMB de ONTAP local

Para que un usuario local pueda acceder a los datos en un servidor CIFS, el usuario debe crear una sesión autenticada.

Debido a que el bloque de mensajes del servidor se basa en sesiones, la identidad del usuario se puede determinar una sola vez cuando se configura la sesión por primera vez. El servidor CIFS utiliza autenticación basada en NTLM al autenticar usuarios locales. Son compatibles tanto NTLMv1 como NTLMv2.

ONTAP utiliza autenticación local en tres casos de uso. Cada caso de uso depende de si la parte del dominio del nombre de usuario (con el formato de DOMINIO\usuario) coincide con el nombre de dominio local del servidor CIFS (el nombre del servidor CIFS):

- La parte del dominio coincide

Los usuarios que proporcionan credenciales de usuario local al solicitar acceso a los datos se autentican localmente en el servidor CIFS.

- La parte del dominio no coincide

ONTAP intenta utilizar la autenticación NTLM con un controlador de dominio del dominio al que pertenece el servidor CIFS. Si la autenticación se realiza correctamente, se completa el inicio de sesión. Si no se realiza correctamente, lo que sucede a continuación depende de por qué la autenticación no se ha realizado correctamente.

Por ejemplo, si el usuario existe en Active Directory pero la contraseña no es válida o ha caducado, ONTAP no intenta utilizar la cuenta de usuario local correspondiente en el servidor CIFS. En su lugar, la autenticación genera errores. Hay otros casos en los que ONTAP utiliza la cuenta local correspondiente en el servidor CIFS, si existe, para la autenticación, aunque los nombres de dominio NetBIOS no coincidan. Por ejemplo, si existe una cuenta de dominio coincidente pero está deshabilitada, ONTAP utiliza la cuenta local correspondiente en el servidor CIFS para la autenticación.

- No se ha especificado la parte del dominio

ONTAP intenta primero la autenticación como usuario local. Si la autenticación como usuario local falla, ONTAP autentica al usuario con una controladora de dominio en el dominio al que pertenece el servidor CIFS.

Una vez que la autenticación de usuario local o de dominio se ha completado correctamente, ONTAP crea un token de acceso de usuario completo, que tiene en cuenta la pertenencia a grupos locales y los privilegios.

Para obtener más información acerca de la autenticación NTLM para usuarios locales, consulte la documentación de Microsoft Windows.

Información relacionada

[Habilitar o deshabilitar la autenticación de usuarios locales en los servidores](#)

Obtenga más información sobre los tokens de acceso de usuario SMB de ONTAP

Cuando un usuario asigna un recurso compartido, se establece una sesión SMB autenticada y se crea un token de acceso de usuario que contiene información acerca del usuario, la pertenencia al grupo del usuario y los privilegios acumulativos, así como el usuario UNIX asignado.

A menos que la funcionalidad esté deshabilitada, la información de grupo y de usuario local también se agrega al token de acceso de usuario. La forma en que se crean los tokens de acceso depende de si el inicio de sesión es para un usuario local o un usuario de dominio de Active Directory:

- Inicio de sesión de usuario local

Aunque los usuarios locales pueden ser miembros de diferentes grupos locales, los grupos locales no pueden ser miembros de otros grupos locales. El token de acceso de usuario local se compone de una unión de todos los privilegios asignados a grupos a los que pertenece un usuario local determinado.

- Inicio de sesión de usuario de dominio

Cuando un usuario de dominio inicia sesión, ONTAP obtiene un token de acceso de usuario que contiene el SID y SID de usuario para todos los grupos de dominio a los que pertenece el usuario. ONTAP utiliza la unión del token de acceso de usuario de dominio con el token de acceso proporcionado por las membresías locales de los grupos de dominio del usuario (si los hay), así como todos los privilegios directos asignados al usuario de dominio o cualquiera de sus pertenencias a grupos de dominio.

Tanto para el inicio de sesión local como para el usuario de dominio, el RID de grupo principal también está configurado para el token de acceso de usuario. El RID predeterminado es `Domain Users` (RID 513). No puede cambiar el valor predeterminado.

El proceso de asignación de nombres de Windows a UNIX y UNIX a Windows sigue las mismas reglas para las cuentas locales y de dominio.



No hay ningún mapeo implícito y automático de un usuario UNIX a una cuenta local. Si es necesario, se debe especificar una regla de asignación explícita mediante los comandos de asignación de nombres existentes.

Obtenga información sobre el uso de SnapMirror en SVM SMB de ONTAP que contienen grupos locales

Debe tener en cuenta las directrices al configurar SnapMirror en los volúmenes que son propiedad de las SVM que contienen grupos locales.

No se pueden utilizar grupos locales en ACE aplicados a archivos, directorios o recursos compartidos replicados por SnapMirror en otra SVM. Si utiliza la función SnapMirror para crear un reflejo de recuperación ante desastres en un volumen en otra SVM y el volumen tiene una ACE para un grupo local, la ACE no es válida en el reflejo. Si los datos se replican en una SVM diferente, estos se cruzan realmente en un dominio local diferente. Los permisos concedidos a los usuarios y grupos locales solo son válidos dentro del ámbito de la SVM en la que se crearon originalmente.

Conozca los efectos de eliminar servidores SMB de ONTAP en usuarios y grupos

El conjunto predeterminado de usuarios y grupos locales se crea cuando se crea un servidor CIFS y está asociado con las máquinas virtuales de almacenamiento (SVM) que alojan el servidor CIFS. Los administradores de SVM pueden crear usuarios y grupos locales en cualquier momento. Debe saber qué sucede con los usuarios locales y los grupos al eliminar el servidor CIFS.

Los usuarios y grupos locales están asociados a las SVM; por lo tanto, no se eliminan cuando los servidores CIFS se eliminan debido a consideraciones de seguridad. Aunque los usuarios y grupos locales no se

eliminan al eliminar el servidor CIFS, sí se ocultan. No se pueden ver ni gestionar usuarios y grupos locales hasta que se vuelva a crear un servidor CIFS en la SVM.



El estado administrativo del servidor CIFS no afecta a la visibilidad de los grupos o usuarios locales.

Aprenda a usar Microsoft Management Console con usuarios y grupos locales de ONTAP SMB

Puede ver información acerca de los usuarios y grupos locales desde la Consola de administración de Microsoft. Con esta versión de ONTAP, no puede realizar otras tareas de administración para usuarios y grupos locales desde la Consola de administración de Microsoft.

Obtenga información sobre cómo revertir clústeres SMB de ONTAP

Si piensa revertir el clúster a una versión de ONTAP que no da soporte a usuarios y grupos locales y se están utilizando grupos y usuarios locales para gestionar los derechos de usuario o el acceso a los archivos, debe tener en cuenta ciertas consideraciones.

- Debido a motivos de seguridad, no se elimina la información sobre usuarios locales, grupos y privilegios configurados cuando ONTAP se revierte a una versión que no admite la funcionalidad de usuarios y grupos locales.
- Al volver a una versión principal anterior de ONTAP, ONTAP no utiliza usuarios ni grupos locales durante la autenticación ni la creación de credenciales.
- Los usuarios y grupos locales no se quitan de las ACL de archivos y carpetas.
- Se deniegan las solicitudes de acceso a archivos que dependen de que se conceda el acceso debido a los permisos concedidos a los usuarios o grupos locales.

Para permitir el acceso, debe volver a configurar los permisos de archivo para permitir el acceso basado en objetos de dominio en lugar de objetos de usuario local y de grupo.

Qué privilegios locales son

Lista de privilegios SMB de ONTAP admitidos

ONTAP tiene un conjunto predefinido de privilegios admitidos. Algunos grupos locales predefinidos tienen algunos de estos privilegios añadidos de forma predeterminada. También puede agregar o quitar privilegios de los grupos predefinidos o crear nuevos usuarios o grupos locales y agregar privilegios a los grupos que creó o a los usuarios y grupos de dominio existentes.

En la siguiente tabla se enumeran los privilegios admitidos en la máquina virtual de almacenamiento (SVM) y se proporciona una lista de los grupos BUILTIN con privilegios asignados:

Nombre del privilegio	Configuración de seguridad predeterminada	Descripción
SeTcbPrivilege	Ninguno	Actuar como parte del sistema operativo
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Realice copias de seguridad de archivos y directorios, anulando cualquier ACL
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restaurar archivos y directorios, anulando cualquier ACL establecer cualquier SID de usuario o grupo válido como propietario del archivo
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Tomar posesión de archivos u otros objetos
SeSecurityPrivilege	BUILTIN\Administrators	Gestionar auditoría Esto incluye ver, volcar y borrar el registro de seguridad.
SeChangeNotifyPrivilege	BUILTIN\Administrators, , , , BUILTIN\Backup Operators BUILTIN\Power Users BUILTIN\Users , Everyone	Comprobación de desvío transversal No es necesario que los usuarios con este privilegio tengan permisos de desplazamiento (x) para recorrer carpetas, vínculos simbólicos o uniones.

Información relacionada

- [Obtenga información sobre la asignación de privilegios](#)
- [Obtenga información sobre cómo configurar la comprobación de recorrido de derivación](#)

Obtenga información sobre la asignación de privilegios SMB de ONTAP

Es posible asignar privilegios directamente a usuarios locales o a usuarios de dominio. También puede asignar usuarios a grupos locales cuyos privilegios asignados coincidan con las capacidades que desea que tengan esos usuarios.

- Puede asignar un conjunto de privilegios a un grupo que cree.

A continuación, agregue un usuario al grupo que tenga los privilegios que desea que tenga ese usuario.

- También puede asignar usuarios locales y usuarios de dominio a grupos predefinidos cuyos privilegios predeterminados coincidan con los privilegios que desea conceder a esos usuarios.

Información relacionada

- [Añada privilegios a usuarios o grupos locales o de dominio](#)
- [Quitar privilegios de usuarios o grupos locales o de dominio](#)
- [Restablecer privilegios para usuarios y grupos locales o de dominio](#)
- [Obtenga información sobre cómo configurar la comprobación de recorrido de derivación](#)

Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores SMB de ONTAP

Hay ciertas pautas que debe tener en cuenta cuando utilice los grupos BUILTIN y la cuenta de administrador local. Por ejemplo, puede cambiar el nombre de la cuenta de administrador local, pero no puede eliminar esta cuenta.

- Se puede cambiar el nombre de la cuenta Administrador, pero no se puede eliminar.
- La cuenta de administrador no se puede quitar del grupo BUILTIN\Administrators.
- Se puede cambiar el nombre de los grupos INTEGRADOS, pero no se pueden eliminar.

Después de cambiar el nombre del grupo BUILTIN, se puede crear otro objeto local con el nombre bien conocido; sin embargo, al objeto se le asigna UN NUEVO RID.

- No hay una cuenta de invitado local.

Información relacionada

[Grupos BUILTIN predefinidos y privilegios predeterminados](#)

Requisitos para las contraseñas de usuarios locales de ONTAP SMB

De manera predeterminada, las contraseñas de usuario local deben cumplir con los requisitos complejos. Los requisitos de complejidad de la contraseña son similares a los que se definen en la directiva de seguridad local de Microsoft Windows.

La contraseña debe cumplir los siguientes criterios:

- Debe tener al menos seis caracteres de longitud
- No se debe contener el nombre de cuenta de usuario
- Debe contener caracteres de al menos tres de las siguientes cuatro categorías:
 - Caracteres en mayúsculas (De La A a la Z)
 - Caracteres en minúscula (de la a a la z)
 - Base de 10 dígitos (de 0 a 9)
 - Caracteres especiales:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Información relacionada

- [Configurar la complejidad de la contraseña para usuarios locales](#)

- [Mostrar información sobre la configuración de seguridad del servidor](#)
- [Cambiar las contraseñas de la cuenta de usuario local](#)

Grupos BUILTIN predefinidos y privilegios SMB de ONTAP predeterminados

Puede asignar la pertenencia de un usuario local o un usuario de dominio a un conjunto predefinido de grupos BUILTIN proporcionados por ONTAP. Los grupos predefinidos tienen privilegios predefinidos asignados.

En la siguiente tabla se describen los grupos predefinidos:

Grupo BUILTIN predefinido	Privilegios predeterminados
BUILTIN\AdministratorsRID 544 Cuando se crea por primera vez, la Administrator cuenta local, con un RID de 500, se convierte automáticamente en miembro de este grupo. Cuando la máquina virtual de almacenamiento (SVM) se une a un dominio, domain\Domain Admins el grupo se añade al grupo. Si la SVM abandona el dominio, domain\Domain Admins el grupo se eliminará del grupo.	• SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
BUILTIN\Power UsersRID 547 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo tienen las siguientes características: • Puede crear y administrar usuarios y grupos locales. • No se pueden agregar ellos mismos ni ningún otro objeto al BUILTIN\Administrators grupo.	SeChangeNotifyPrivilege
BUILTIN\Backup OperatorsRID 551 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo pueden anular los permisos de lectura y escritura en archivos o carpetas si se abren con la intención de copia de seguridad.	• SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege

Grupo BUILTIN predefinido	Privilegios predeterminados
BUILTIN\UsersRID 545 Cuando se crea por primera vez, este grupo no tiene ningún miembro (además del Authenticated Users grupo especial implícito). Cuando la SVM se une a un dominio, el domain\Domain Users grupo se añade a este grupo. Si la SVM abandona el dominio, domain\Domain Users el grupo se eliminará de este grupo.	SeChangeNotifyPrivilege
EveryoneSID S-1-1-0 Este grupo incluye a todos los usuarios, incluidos invitados (pero no usuarios anónimos). Este es un grupo implícito con una membresía implícita.	SeChangeNotifyPrivilege

Información relacionada

- [Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores](#)
- [Lista de privilegios compatibles](#)
- [Obtenga información sobre cómo configurar la comprobación de recorrido de derivación](#)

Habilite o deshabilite la funcionalidad de grupos y usuarios locales

Obtenga información sobre la funcionalidad de los usuarios y grupos SMB locales de ONTAP

Antes de poder utilizar usuarios y grupos locales para controlar el acceso a los datos del estilo de seguridad NTFS, se debe habilitar la funcionalidad de usuario local y grupo. Además, si desea utilizar usuarios locales para la autenticación SMB, se debe habilitar la funcionalidad de autenticación de usuarios locales.

La funcionalidad de grupos y usuarios locales y la autenticación de usuarios locales están habilitadas de forma predeterminada. Si no están habilitadas, debe habilitarlas para poder configurar y utilizar usuarios y grupos locales. La funcionalidad de grupos y usuarios locales se puede deshabilitar en cualquier momento.

Además de deshabilitar explícitamente la funcionalidad de grupo y usuario local, ONTAP deshabilita la funcionalidad de grupo y usuario local si algún nodo del clúster se revierte a una versión de ONTAP que no admite la funcionalidad. La funcionalidad de usuario local y de grupo no está habilitada hasta que todos los nodos del clúster ejecuten una versión de ONTAP que la admita.

Información relacionada

- [Modifique las cuentas de usuario local](#)
- [Modificar grupos locales](#)
- [Añada privilegios a usuarios o grupos locales o de dominio](#)

Habilitar o deshabilitar usuarios y grupos locales en servidores SMB de ONTAP

Puede habilitar o deshabilitar usuarios y grupos locales para el acceso SMB en

máquinas virtuales de almacenamiento (SVM). La funcionalidad de grupos y usuarios locales está activada de forma predeterminada.

Acerca de esta tarea

Puede usar usuarios y grupos locales al configurar los permisos de archivos NTFS y compartidos de SMB, y puede usar, opcionalmente, usuarios locales para la autenticación al crear una conexión SMB. Para usar usuarios locales para la autenticación, también debe habilitar la opción de autenticación de grupos y usuarios locales.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que los grupos y usuarios locales sean...	Introduzca el comando...
Activado	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true</code>
Deshabilitado	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false</code>

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la funcionalidad de grupos y usuarios locales en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- [Habilitar o deshabilitar la autenticación de usuarios locales en los servidores](#)
- [Habilite o deshabilite cuentas de usuario locales](#)

Habilitar o deshabilitar la autenticación de usuarios locales en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la autenticación de usuario local para el acceso SMB en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es permitir la

autenticación de usuario local, que resulta útil cuando la SVM no puede ponerse en contacto con un controlador de dominio o si decide no utilizar controles de acceso a nivel de dominio.

Antes de empezar

La funcionalidad de grupos y usuarios locales debe estar habilitada en el servidor CIFS.

Acerca de esta tarea

Es posible habilitar o deshabilitar la autenticación de usuario local en cualquier momento. Si desea usar usuarios locales para la autenticación al crear una conexión SMB, también debe habilitar la opción de grupos y usuarios locales del servidor CIFS.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la autenticación local sea...	Introduzca el comando...
Activado	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
Deshabilitado	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la autenticación de usuario local en SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- [Obtenga más información sobre la autenticación de usuarios locales](#)
- [Habilitar o deshabilitar usuarios y grupos locales en servidores](#)

Permite gestionar cuentas de usuario local

Modificar cuentas de usuario SMB locales de ONTAP

Puede modificar una cuenta de usuario local si desea cambiar el nombre completo o la descripción de un usuario existente y si desea habilitar o deshabilitar la cuenta de usuario. También puede cambiar el nombre de una cuenta de usuario local si el nombre del usuario está en peligro o si se necesita un cambio de nombre con fines administrativos.

Si desea...	Introduzca el comando...
Modifique el nombre completo del usuario local	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -full-name <i>text</i></code> Si el nombre completo contiene un espacio, debe estar entre comillas dobles.
Modifique la descripción del usuario local	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description <i>text</i></code> Si la descripción contiene un espacio, debe estar entre comillas dobles.
Habilite o deshabilite la cuenta de usuario local	<code>`vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is -account-disabled {true</code>
<code>false}`</code>	Cambie el nombre de la cuenta de usuario local

Ejemplo

En el siguiente ejemplo, se cambia el nombre del usuario local «'CIFS_SERVER\sue'» a «'CIFS_SERVER\sue_new'» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name  
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Habilitar o deshabilitar cuentas de usuario SMB de ONTAP locales

Es posible habilitar una cuenta de usuario local si desea que el usuario pueda acceder a los datos contenidos en la máquina virtual de almacenamiento (SVM) a través de una conexión de SMB. También puede deshabilitar una cuenta de usuario local si no desea que ese usuario acceda a los datos de SVM mediante SMB.

Acerca de esta tarea

Para habilitar un usuario local, debe modificar la cuenta de usuario.

Paso

1. Ejecute la acción adecuada:

Si desea...	Introduzca el comando...
Habilite la cuenta de usuario	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false</pre>
Desactive la cuenta de usuario	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

Cambiar las contraseñas de las cuentas de usuario locales de ONTAP SMB

Es posible cambiar la contraseña de la cuenta de un usuario local. Esto puede ser útil si la contraseña del usuario está en peligro o si el usuario ha olvidado la contraseña.

Paso

1. Cambie la contraseña realizando la acción adecuada:

```
vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name
```

Ejemplo

En el siguiente ejemplo, se establece la contraseña del usuario local "CIFS_SERVER\sue" asociada con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user -name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

Información relacionada

[Configurar la complejidad de la contraseña para usuarios locales](#)

[Mostrar información sobre la configuración de seguridad del servidor](#)

Mostrar información sobre los usuarios locales de ONTAP SMB

Puede mostrar una lista de todos los usuarios locales en un formulario de resumen. Si desea determinar qué configuración de cuenta está configurada para un usuario específico, puede mostrar información detallada de la cuenta para ese usuario, así como la información de la cuenta para varios usuarios. Esta información puede ayudarle a determinar si necesita modificar la configuración de un usuario y también a resolver problemas de autenticación o acceso a archivos.

Acerca de esta tarea

Nunca se muestra información sobre la contraseña de un usuario.

Paso

- 1. Ejecute una de las siguientes acciones:

Si desea...	Introduzca el comando...
Mostrar información sobre todos los usuarios de la máquina virtual de almacenamiento (SVM)	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
Muestra información detallada de la cuenta de un usuario	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

Hay otros parámetros opcionales que puede elegir cuando ejecuta el comando. Obtenga más información sobre `vserver cifs` en el ["Referencia de comandos del ONTAP"](#).

Ejemplo

El siguiente ejemplo muestra información sobre todos los usuarios locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator      James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue                Sue   Jones
```

Mostrar información sobre las membresías del grupo SMB de ONTAP para usuarios locales

Puede mostrar información sobre los grupos locales a los que pertenece un usuario local. Puede utilizar esta información para determinar qué acceso debe tener el usuario a los archivos y carpetas. Esta información puede ser útil para determinar qué derechos de acceso debe tener el usuario a los archivos y carpetas o al solucionar problemas de acceso a archivos.

Acerca de esta tarea

Puede personalizar el comando para que muestre solo la información que desea ver.

Paso

- 1. Ejecute una de las siguientes acciones:

Si desea...	Introduzca el comando...
Muestra información de pertenencia de usuario local para un usuario local específico	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Mostrar información de pertenencia al usuario local para el grupo local del que forma parte este usuario local	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Mostrar información de pertenencia al usuario para los usuarios locales que están asociados a una máquina virtual de almacenamiento (SVM) especificada	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Mostrar información detallada para todos los usuarios locales en una SVM especificada	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

Ejemplo

En el siguiente ejemplo se muestra la información de pertenencia de todos los usuarios locales de SVM vs1; el usuario «'CIFS_SERVER\Administrator'» es miembro del grupo «'BUILTIN\Administrators'» y «'CIFS_SERVER\sue'» es miembro del grupo «'CIFS_SERVER\g1'»:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
```

Vserver	User Name	Membership
vs1	CIFS_SERVER\Administrator	BUILTIN\Administrators
	CIFS_SERVER\sue	CIFS_SERVER\g1

Eliminar cuentas de usuario SMB de ONTAP locales

Es posible eliminar cuentas de usuario locales de la máquina virtual de almacenamiento (SVM) si ya no son necesarias para la autenticación local de SMB en el servidor CIFS o para determinar los derechos de acceso a los datos incluidos en la SVM.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar usuarios locales:

- El sistema de archivos no se ha modificado.

Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este usuario no están ajustados.

- Todas las referencias a los usuarios locales se eliminan de las bases de datos de pertenencia y privilegios.
- No se pueden eliminar los usuarios estándar conocidos, como el Administrador.

Pasos

- 1. Determine el nombre de la cuenta de usuario local que desea eliminar: `vserver cifs users-and-groups local-user show -vserver vserver_name`
- 2. Elimine el usuario local: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
- 3. Compruebe que se ha eliminado la cuenta de usuario: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se elimina el usuario local "CIFS_SERVER\sue" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator    James Smith              Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue    Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                Full Name                Description
-----  -
vs1          CIFS_SERVER\Administrator    James Smith              Built-in administrator
account
```

Administrar grupos locales

Modificar grupos SMB locales de ONTAP

Puede modificar los grupos locales existentes cambiando la descripción de un grupo local existente o cambiando el nombre del grupo.

Si desea...	Usar el comando...
Modifique la descripción del grupo local	<code>vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text</code> Si la descripción contiene un espacio, debe estar entre comillas dobles.

Si desea...	Usar el comando...
Cambie el nombre del grupo local	<code>vserver cifs users-and-groups local-group rename -vserver <i>vserver_name</i> -group-name <i>group_name</i> -new-group-name <i>new_group_name</i></code>

Ejemplos

En el ejemplo siguiente se cambia el nombre del grupo local "CIFS_SERVER\engineering" a "CIFS_SERVER\engineering_new":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

En el siguiente ejemplo se modifica la descripción del grupo local "CIFS_SERVER\engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Mostrar información sobre los grupos locales de SMB de ONTAP

Es posible mostrar una lista de todos los grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) específica. Esta información puede ser útil para solucionar problemas de acceso a los archivos en la SVM o problemas de derechos de usuario (privilegios) en la SVM.

Paso

1. Ejecute una de las siguientes acciones:

Si desea información acerca de...	Introduzca el comando...
Todos los grupos locales del clúster	<code>vserver cifs users-and-groups local-group show</code>
Todos los grupos locales en la SVM	<code>vserver cifs users-and-groups local-group show -vserver <i>vserver_name</i></code>

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs` en el ["Referencia de comandos del ONTAP"](#).

Ejemplo

En el siguiente ejemplo, se muestra información sobre todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative privileges
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

Gestionar la pertenencia a un grupo SMB de ONTAP local

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

Acerca de esta tarea

Directrices para agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- El grupo local debe existir antes de poder añadir un usuario.
- El usuario debe existir antes de poder agregar el usuario a un grupo local.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, Data ONTAP debe poder resolver el nombre a un SID.

Directrices para eliminar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- El grupo del que desea quitar un miembro debe existir.
- ONTAP debe poder resolver los nombres de los miembros que desea quitar del grupo a un SID correspondiente.

Paso

1. Agregar o quitar un miembro de un grupo.

Si desea...	A continuación, se usa el comando...
Agregar un miembro a un grupo	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para agregarlos al grupo local especificado.
Quitar un miembro de un grupo	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para eliminarlos del grupo local especificado.

En el siguiente ejemplo, se agrega un usuario local "MB_SERVER\sue" y un grupo de dominios "AD_DOM\dom_eng" al grupo local "MB_SERVER\engineering" en SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

En el siguiente ejemplo se eliminan los usuarios locales «MB_SERVER\sue» y «MB_SERVER\james» del grupo local «MB_SERVER\engineering» de SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Información relacionada

[Muestra información acerca de los miembros de los grupos locales](#)

Mostrar información de ONTAP SMB sobre los miembros de los grupos locales

Es posible mostrar una lista de todos los miembros de grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ser útil para solucionar problemas de acceso a archivos o problemas de derechos de usuario (privilegios).

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de...	Introduzca el comando...
Miembros de todos los grupos locales del cluster	<code>vserver cifs users-and-groups local-group show-members</code>
Miembros de todos los grupos locales en la SVM	<code>vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i></code>

Ejemplo

En el siguiente ejemplo, se muestra información acerca de los miembros de todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
```

Vserver	Group Name	Members
vs1	BUILTIN\Administrators	CIFS_SERVER\Administrator AD_DOMAIN\Domain Admins AD_DOMAIN\dom_grp1
	BUILTIN\Users	AD_DOMAIN\Domain Users AD_DOMAIN\dom_usr1
	CIFS_SERVER\engineering	CIFS_SERVER\james

Eliminar grupos SMB locales de ONTAP

Es posible eliminar un grupo local de la máquina virtual de almacenamiento (SVM) si ya no es necesario para determinar los derechos de acceso a los datos asociados con esa SVM o si ya no es necesario para asignar los derechos de usuario (privilegios) de SVM a los miembros del grupo.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar grupos locales:

- El sistema de archivos no se ha modificado.
Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este grupo no se ajustan.
- Si el grupo no existe, se devuelve un error.
- El grupo especial *Everyone* no se puede eliminar.
- Los grupos integrados como *BUILTIN\Administrators* *BUILTIN\Users* no se pueden eliminar.

Pasos

1. Determine el nombre del grupo local que desea eliminar. Para ello, muestre la lista de grupos locales en la SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`

2. Elimine el grupo local: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Compruebe que el grupo se ha suprimido: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se elimina el grupo local "CIFS_SERVER\sales" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
	privileges	
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

```
cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
	privileges	
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	

Actualizar los nombres de usuarios y grupos del dominio SMB de ONTAP en las bases de datos locales

Puede agregar usuarios y grupos de dominio a los grupos locales de un servidor CIFS. Estos objetos de dominio se registran en bases de datos locales en el clúster. Si se cambia el nombre de un objeto de dominio, las bases de datos locales deben actualizarse manualmente.

Acerca de esta tarea

Debe especificar el nombre de la máquina virtual de almacenamiento (SVM) en la que desea actualizar los nombres de dominio.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`

2. Ejecute la acción adecuada:

Si desea actualizar usuarios y grupos de dominio y...	Se usa este comando...
Muestra usuarios y grupos de dominio que se han actualizado correctamente y que no se han podido actualizar	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>
Muestra los usuarios y grupos de dominio que se han actualizado correctamente	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Muestra sólo los usuarios y grupos de dominio que no se pueden actualizar	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Suprimir toda la información de estado acerca de las actualizaciones	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

En el siguiente ejemplo se actualizan los nombres de los usuarios y grupos de dominio asociados con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Para la última actualización, hay una cadena de nombres dependiente que se debe actualizar:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:          EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:          EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:          EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:          Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

Gestione los privilegios locales

Agregar privilegios a usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar los derechos de usuario para usuarios o grupos locales o de dominio mediante la adición de privilegios. Los privilegios agregados anulan los privilegios predeterminados asignados a cualquiera de estos objetos. Esto proporciona una seguridad mejorada al permitirle personalizar qué privilegios tiene un usuario o grupo.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio al que se añadirán privilegios.

Acerca de esta tarea

Al agregar un privilegio a un objeto se reemplazan los privilegios predeterminados para ese usuario o grupo. Al añadir un privilegio, no se quitan los privilegios añadidos anteriormente.

Debe tener en cuenta lo siguiente al agregar privilegios a usuarios o grupos locales o de dominio:

- Puede añadir uno o varios privilegios.
- Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Añada una o más Privileges a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Compruebe que se aplican los Privileges deseados al objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplo

En el siguiente ejemplo, se añaden los privilegios «ShebPrivilege» y «SeeTakeOwnershipPrivilege» al usuario «CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Eliminar privilegios de usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar derechos de usuario para usuarios o grupos locales o de dominio eliminando privilegios. Esto proporciona una seguridad mejorada al permitirle

personalizar los privilegios máximos que tienen los usuarios y los grupos.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al quitar privilegios de usuarios o grupos locales o de dominio, debe tener en cuenta lo siguiente:

- Puede eliminar uno o varios privilegios.
- Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Quite una o más Privileges de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verifique que el Privileges deseado se haya eliminado del objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplo

En el siguiente ejemplo se eliminan los privilegios «DeeTcbPrivilege» y «SeeTakeOwnershipPrivilege» del usuario «CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue     -
```

Restablecer privilegios para usuarios y grupos locales o de dominio de ONTAP SMB

Es posible restablecer privilegios para los grupos y usuarios locales o de dominio. Esto puede ser útil si ha realizado modificaciones a los privilegios de un usuario o grupo local o de dominio y esas modificaciones ya no se desean ni se necesitan.

Acerca de esta tarea

Al restablecer los privilegios de un usuario o grupo local o de dominio, se quitan todas las entradas de privilegios de ese objeto.

Pasos

1. Restablezca la Privileges en un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Compruebe que los Privileges se han restablecido en el objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplos

En el siguiente ejemplo, se restablecen los privilegios para el usuario «'CIFS_SERVER\sue'» en la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) vs1. De forma predeterminada, los usuarios normales no tienen privilegios asociados a sus cuentas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

En el ejemplo siguiente se restablecen los privilegios para el grupo "BUILTIN\Administrators", eliminando de forma efectiva la entrada de privilegios:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                                SeSecurityPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Mostrar información sobre las anulaciones de privilegios SMB de ONTAP

Puede mostrar información acerca de los privilegios personalizados asignados a cuentas o grupos de usuarios locales o de dominio. Esta información le ayuda a determinar si se aplican los derechos de usuario deseados.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de...	Introduzca este comando...
Privilegios personalizados para todos los grupos y usuarios locales y de dominio en la máquina virtual de almacenamiento (SVM)	<pre>vserver cifs users-and-groups privilege show -vserver vserver_name</pre>
Privilegios personalizados para un dominio o un grupo y usuario local específicos de la SVM	<pre>vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name</pre>

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs users-and-groups privilege show` en el ["Referencia de comandos del ONTAP"](#).

Ejemplo

El siguiente comando muestra todos los privilegios asociados explícitamente con los usuarios y grupos locales o de dominio para SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
-----	-----	-----
vs1	BUILTIN\Administrators	SeTakeOwnershipPrivilege SeRestorePrivilege
vs1	CIFS_SERVER\sue	SeTcbPrivilege SeTakeOwnershipPrivilege

Configurar la comprobación de recorrido de derivación

Obtenga información sobre cómo configurar la comprobación de travesía de derivación de SMB de ONTAP

La comprobación de recorrido de omisión es un derecho de usuario (también conocido como *Privilege*) que determina si un usuario puede recorrer todos los directorios de la ruta de acceso a un archivo incluso si el usuario no tiene permisos en el directorio de recorrido. Debe comprender lo que sucede al permitir o dejar de permitir la comprobación de recorrido por omisión, y cómo configurar la comprobación de recorrido por omisión para los usuarios en máquinas virtuales de almacenamiento (SVM).

Qué sucede cuando se permite o se despermite la comprobación de recorrido de derivación

- Si se permite, cuando un usuario intenta acceder a un archivo, ONTAP no comprueba el permiso Traverse para los directorios intermedios al determinar si se concede o deniega el acceso al archivo.
- Si no se permite, ONTAP comprueba el permiso recorrer (ejecutar) para todos los directorios de la ruta de acceso al archivo.

Si alguno de los directorios intermedios no tiene el "X" (permiso de desplazamiento), ONTAP niega el acceso al archivo.

Configurar la comprobación de recorrido de derivación

Puede configurar la comprobación de recorrido de desvío mediante la interfaz de línea de comandos de ONTAP o mediante la configuración de directivas de grupo de Active Directory con este derecho de usuario.

```
`SeChangeNotifyPrivilege`El privilegio controla si los usuarios pueden omitir la comprobación transversal.
```

- Si se la agrega a los usuarios o grupos SMB locales en la SVM o a usuarios o grupos de dominio, permite omitir el control transversal.
- Si lo elimina de usuarios o grupos SMB locales en la SVM o de usuarios o grupos de dominio, no permite omitir la comprobación cruzada.

De forma predeterminada, los siguientes grupos BUILTIN de la SVM tienen derecho a omitir la comprobación de recorrido:

- BUILTIN\Administrators
- BUILTIN\Power Users
- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

Si no desea permitir a los miembros de uno de estos grupos omitir la comprobación de recorrido, debe quitar este privilegio del grupo.

Debe tener en cuenta lo siguiente al configurar la comprobación de derivación cruzada de usuarios y grupos de SMB locales en la SVM mediante la CLI:

- Si desea permitir que los miembros de un grupo local o de dominio personalizado omitan la comprobación transversal, debe agregar el `SeChangeNotifyPrivilege` privilegio a ese grupo.
- Si desea permitir que un usuario local o de dominio individual omita la comprobación transversal y que ese usuario no sea miembro de un grupo con ese privilegio, puede agregar el `SeChangeNotifyPrivilege` privilegio a esa cuenta de usuario.
- Puede desactivar la comprobación transversal de omisión para usuarios o grupos locales o de dominio eliminando el `SeChangeNotifyPrivilege` privilegio en cualquier momento.



Para desactivar la comprobación de bypass travers para usuarios o grupos locales o de dominio especificados, también debe eliminar el SeChangeNotifyPrivilege privilegio del Everyone grupo.

Información relacionada

- [Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)
- [No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)
- [Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes](#)
- [Crear listas de control de acceso a recursos compartidos](#)
- [Acceso seguro a archivos mediante Storage-Level Access Guard](#)
- [Lista de privilegios compatibles](#)
- [Añada privilegios a usuarios o grupos locales o de dominio](#)

Permitir que los usuarios o grupos omitan la verificación del recorrido del directorio SMB de ONTAP

Si desea que un usuario pueda recorrer todos los directorios de la ruta a un archivo, aunque el usuario no tenga permisos en un directorio cruzado, puede añadir el SeChangeNotifyPrivilege privilegio a grupos o usuarios locales de SMB en máquinas virtuales de almacenamiento (SVM). De forma predeterminada, los usuarios pueden omitir la comprobación de recorrido del directorio.

Antes de empezar

- Debe haber un servidor SMB en la SVM.
- Debe habilitarse la opción del servidor SMB para los usuarios locales y los grupos.
- El usuario o grupo local o de dominio al que se SeChangeNotifyPrivilege agregará el privilegio debe existir ya.

Acerca de esta tarea

Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Active la comprobación de desvío mediante la adición SeChangeNotifyPrivilege del privilegio a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

El valor del `-user-or-group-name` parámetro es un usuario o un grupo local, o un usuario o un grupo de dominio.

2. Compruebe que el usuario o grupo especificado tiene activada la comprobación de desvío de desvío: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplo

El siguiente comando permite a los usuarios que pertenecen al grupo «EJEMPLO\eng» omitir la comprobación de desplazamiento de directorios agregando el SeChangeNotifyPrivilege privilegio al grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

Información relacionada

[No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)

No permitir que usuarios o grupos omitan la comprobación del recorrido del directorio SMB de ONTAP

Si no desea que un usuario recorra todos los directorios de la ruta a un archivo porque el usuario no tiene permisos en el directorio cruzado, puede quitar el SeChangeNotifyPrivilege privilegio de los usuarios o grupos locales de SMB en las máquinas virtuales de almacenamiento (SVM).

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. No permitir la comprobación de desvío: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

El comando quita SeChangeNotifyPrivilege el privilegio del usuario o grupo local o de dominio que se especifique con el valor del `-user-or-group-name name` parámetro.

2. Compruebe que el usuario o grupo especificado tiene desactivada la comprobación de desvío: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplo

El siguiente comando evita que los usuarios que pertenecen al grupo "EXAMPLE\eng" pasen por alto la comprobación de recorrido del directorio:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\eng	SeChangeNotifyPrivilege

```
cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\eng	-

Información relacionada

[Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)

Muestra información acerca de las políticas de auditoría y seguridad de archivos

Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos SMB de ONTAP

Puede mostrar información sobre la seguridad de los archivos y directorios contenidos en volúmenes en máquinas virtuales de almacenamiento (SVM). Puede mostrar información sobre las políticas de auditoría en los volúmenes de FlexVol. Si se configura, se puede mostrar información acerca de las opciones de seguridad Protección del acceso a nivel de almacenamiento y Control de acceso dinámico en volúmenes de FlexVol.

Mostrar información acerca de la seguridad de archivos

Puede visualizar la información sobre la seguridad de los archivos aplicada a los datos contenidos en volúmenes y qtrees (para volúmenes FlexVol) con los siguientes estilos de seguridad:

- NTFS
- UNIX
- Mixto

Visualización de información acerca de las directivas de auditoría

Puede mostrar información sobre las políticas de auditoría para auditar eventos de acceso en los volúmenes FlexVol mediante los siguientes protocolos NAS:

- SMB (todas las versiones)
- NFSv4.x

Mostrar información acerca de la seguridad de la protección de acceso a nivel de almacenamiento (SLAG)

La seguridad de protección de acceso a nivel de almacenamiento se puede aplicar en volúmenes de FlexVol y objetos de qtree con los siguientes estilos de seguridad:

- NTFS
- Mixto
- UNIX (si se configura un servidor CIFS en la SVM que contiene el volumen)

Mostrar información acerca de la seguridad del control de acceso dinámico (DAC)

La seguridad de control de acceso dinámico se puede aplicar a un objeto dentro de un volumen FlexVol con los siguientes estilos de seguridad:

- NTFS
- Mixto (si el objeto tiene seguridad efectiva NTFS)

Información relacionada

- [Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard](#)
- [Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores](#)

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad NTFS

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes de estilo de seguridad NTFS, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de los atributos dos. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Debido a que los volúmenes y qtrees de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.
- Se muestra la salida de ACL para archivos y carpetas con seguridad NTFS.
- Como la seguridad de Access Guard a nivel de almacenamiento se puede configurar en el volumen raíz o en el qtree, la salida de un volumen o una ruta de qtree en la que se configure la protección de acceso a nivel de almacenamiento puede mostrar tanto ACL de archivos normales como ACL de Storage-Level Access Guard.
- El resultado también muestra información acerca de los ACE de control de acceso dinámico si el Control de acceso dinámico está configurado para la ruta de acceso de archivo o directorio indicada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información...	Introduzca el siguiente comando...
En forma de resumen	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con detalle ampliado	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/vol4` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

                Vserver: vs1
                File Path: /vol4
            File Inode Number: 64
                Security Style: ntfs
                Effective Style: ntfs
                DOS Attributes: 10
        DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
                Unix Group Id: 0
                Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                ACLs: NTFS Security Descriptor
                    Control:0x8004
                    Owner:BUILTIN\Administrators
                    Group:BUILTIN\Administrators
                    DACL - ACEs
                    ALLOW-Everyone-0x1f01ff
                    ALLOW-Everyone-0x10000000-
```

OI|CI|IO

En el siguiente ejemplo, se muestra la información de seguridad con máscaras expandidas sobre la ruta de `/data/engineering` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path  
/data/engineering -expand-mask true
```

```

                Vserver: vs1
                File Path: /data/engineering
            File Inode Number: 5544
```

```

Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... .... = SACL Inherited
    .... .0.. .... = DACL Inherited
    .... ..0. .... = SACL Inherit Required
    .... ...0 .... = DACL Inherit Required
    .... .... ..0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

    Owner:BUILTIN\Administrators
    Group:BUILTIN\Administrators
    DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    0... .... =
Generic Read
    .0.. .... =
Generic Write
    ..0. .... =
Generic Execute
    ...0 .... =

```

Generic All	0.....	=
System Security	1.....	=
Synchronize	1.....	=
Write Owner	1.....	=
Write DAC	1.....	=
Read Control	1.....	=
Delete	1.....	=
Write Attributes	1.....	=
Read Attributes	1.....	=
Delete Child	1.....	=
Execute	1.....	=
Write EA	1.....	=
Read EA	1.....	=
Append	1.....	=
Write	1.....	=
Read	1.....	=
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0.....	=
Generic Write	.0.....	=
Generic Execute	..0.....	=
Generic All	...1.....	=
System Security	0.....	=
Synchronize	0.....	=

Write Owner	0..... =
Write DAC	0..... =
Read Control	0..... =
Delete	0..... =
Write Attributes	0..... =
Read Attributes	0..... =
Delete Child	0..... =
Execute	0..... =
Write EA	0..... =
Read EA	0..... =
Append	0..... =
Write	0..... =
Read	0..... =

En el siguiente ejemplo, se muestra información de seguridad, incluida la información de seguridad de Storage-Level Access Guard, del volumen con la ruta /datavol1 en SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Información relacionada

- [Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad](#)
- [Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX](#)

Mostrar información sobre la seguridad de los archivos SMB de ONTAP en volúmenes de estilo de seguridad mixto

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes mixtos de estilo de seguridad, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y carpetas que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.
- El nivel superior de un volumen mixto de estilo de seguridad puede tener una seguridad efectiva de UNIX o NTFS.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, La salida de un volumen o una ruta de qtree en la que se configure Storage-Level Access Guard podría mostrar tanto los permisos de archivos UNIX como las ACL de Storage-Level Access Guard.
- Si la ruta de acceso introducida en el comando es a datos con seguridad efectiva de NTFS, el resultado también muestra información acerca de ACE de Control de acceso dinámico si Control de acceso dinámico está configurado para el archivo o la ruta de acceso de directorio dada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información...	Introduzca el siguiente comando...
En forma de resumen	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con detalle ampliado	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Ejemplos

El siguiente ejemplo muestra la información de seguridad sobre la ruta de /projects SVM VS1 en formato de máscara expandida. Esta ruta mixta de estilo de seguridad tiene una seguridad efectiva de UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```

        Vserver: vs1
        File Path: /projects
    File Inode Number: 78
        Security Style: mixed
    Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ....0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de /data SVM VS1. Esta ruta mixta de estilo de seguridad tiene una seguridad NTFS efectiva.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

En el ejemplo siguiente se muestra información de seguridad sobre el volumen en la ruta de /datavol5 SVM VS1. El nivel superior de este volumen mixto de estilo de seguridad ofrece una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vservers security file-directory show -vservers vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

Información relacionada

- [Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS](#)
- [Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX](#)

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad UNIX

Puede mostrar información acerca de la seguridad de archivos y directorios en los volúmenes de estilo de seguridad de UNIX, incluidos los estilos de seguridad y los estilos

de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuyo archivo o información de seguridad de directorio desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan permisos de archivos UNIX, ya sea bits de modo o ACL de NFSv4 al determinar los derechos de acceso a los archivos.
- La salida de ACL se muestra solo para los archivos y las carpetas con seguridad de NFSv4.

Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida de ACL no se aplican en el caso de los descriptores de seguridad de NFSv4.

Sólo son significativos para los descriptores de seguridad NTFS.

- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información...	Introduzca el siguiente comando...
En forma de resumen	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con detalle ampliado	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/home SVM VS1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

El siguiente ejemplo muestra la información de seguridad sobre la ruta de /home SVM VS1 en formato de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

Información relacionada

- [Mostrar información sobre la seguridad de los archivos en volúmenes de estilo de seguridad](#)
- [Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad](#)

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NTFS en volúmenes SMB FlexVol

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.
- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

Paso

1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información...	Introduzca el siguiente comando...
En forma de resumen	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Como una lista detallada	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Ejemplos

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/corp` en SVM VS1. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/datavol1` en SVM VS1. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-Level Access

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes SMB FlexVol

Puede mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes de FlexVol mediante la interfaz de línea de comandos de ONTAP, incluidos los estilos de seguridad y los estilos de seguridad efectivos, qué permisos se aplican e información sobre las listas de control de acceso del sistema (SACL). Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o directorios cuya información de auditoría desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan NFSv4 SACL para las políticas de auditoría.
- Los archivos y directorios de un volumen de estilo de seguridad mixto que sea de estilo de seguridad UNIX pueden hacer que se les apliquen las políticas de auditoría de NFSv4.

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen con estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que contenga o no SACL de NFSv4.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, Los resultados de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard pueden mostrar tanto el archivo NFSv4 normal como las SACL de directorio y las SACL de Storage-Level Access Guard.
- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Pasos

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información...	Introduzca el siguiente comando...
En forma de resumen	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>

Si desea mostrar información...	Introduzca el siguiente comando...
Con detalle ampliado	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de /lab SVM VS1. Esta ruta de seguridad de UNIX tiene un SACL de NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
File Inode Number: 288
      Security Style: unix
Effective Style: unix
      DOS Attributes: 11
DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
Control:0x8014
      SACL - ACEs
      SUCCESSFUL-S-1-520-0-0xf01ff-SA
      FAILED-S-1-520-0-0xf01ff-FA
      DACL - ACEs
      ALLOW-S-1-520-1-0xf01ff
```

Aprenda a mostrar información sobre políticas de auditoría y seguridad de archivos SMB de ONTAP

Puede utilizar el carácter comodín (*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de acceso determinada o de un volumen raíz.

El carácter comodín () **se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios. Si desea mostrar información de un archivo o directorio concreto denominado «»», deberá proporcionar la ruta completa dentro de comillas dobles («»")**.

Ejemplo

El siguiente comando con carácter comodín muestra la información de todos los archivos y directorios debajo

de la ruta de /1/ SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /1/*
```

```

    Vserver: vs1
    File Path: /1/1
    Security Style: mixed
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

    Vserver: vs1
    File Path: /1/1/abc
    Security Style: mixed
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

El siguiente comando muestra la información de un archivo llamado "*" bajo la ruta de /vol1/a SVM VS1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
        Unix User Id: 1002  
        Unix Group Id: 65533  
        Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
        Control:0x8014  
        SACL - ACEs  
        AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
        DACL - ACEs  
        ALLOW-EVERYONE@-0x1f00a9-FI|DI  
        ALLOW-OWNER@-0x1f01ff-FI|DI  
        ALLOW-GROUP@-0x1200a9-IG
```

Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI

Comandos ONTAP para administrar la seguridad de archivos NTFS de SMB, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento

Puede gestionar la seguridad de archivos NTFS, políticas de auditoría de NTFS y Storage-Level Access Guard en máquinas virtuales de almacenamiento (SVM) mediante la interfaz de línea de comandos.

Puede gestionar las políticas de auditoría y seguridad de archivos NTFS desde clientes SMB o mediante la CLI. Sin embargo, al utilizar la interfaz de línea de comandos para configurar las políticas de seguridad de los archivos y de auditoría, no es necesario utilizar un cliente remoto para gestionar la seguridad de los archivos. El uso de la CLI puede reducir significativamente el tiempo que lleva aplicar la seguridad en muchos archivos y carpetas mediante un único comando.

Puede configurar la protección de acceso al nivel de almacenamiento, que es otra capa de seguridad aplicada por ONTAP a los volúmenes de SVM. Storage-Level Access Guard se aplica a los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se aplica la protección de acceso a nivel de almacenamiento.

El protector de acceso a nivel de almacenamiento se puede configurar y gestionar solo desde la interfaz de línea de comandos de ONTAP. No se puede gestionar la configuración de Access Guard en el nivel de almacenamiento desde clientes SMB. Además, si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad Storage-Level Access Guard. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un administrador de sistema (Windows o UNIX). Por lo tanto, Storage-Level Access Guard ofrece una capa adicional de seguridad para el acceso a los datos que el administrador de almacenamiento establece y gestiona independientemente.



Aunque solo se admiten permisos de acceso NTFS para Storage-Level Access Guard, ONTAP puede realizar comprobaciones de seguridad para acceder a través de NFS a datos en volúmenes donde se aplica Storage-Level Access Guard si el usuario UNIX se asigna a un usuario de Windows en la SVM propietaria del volumen.

Volúmenes de estilo de seguridad de NTFS

Todos los archivos y carpetas contenidos en qtrees y volúmenes de estilo de seguridad NTFS tienen una seguridad efectiva de NTFS. Puede utilizar `vserver security file-directory` la familia de comandos para implementar los siguientes tipos de seguridad en volúmenes de estilo de seguridad NTFS:

- Los permisos de archivo y las políticas de auditoría a los archivos y las carpetas que contiene el volumen
- Seguridad para proteger el acceso al nivel de almacenamiento en los volúmenes

Volúmenes mixtos de estilo de seguridad

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener algunos archivos y carpetas con seguridad efectiva de UNIX y usar permisos de archivos de UNIX, bits de modo o ACL de NFSv4.x y políticas de auditoría de NFSv4.x, y algunos archivos y carpetas que tengan seguridad efectiva de NTFS y usen permisos de archivos NTFS y políticas de auditoría. Puede utilizar `vserver security file-directory` la familia de comandos para aplicar los siguientes tipos de seguridad a los datos mixtos de estilo de seguridad:

- Permisos de archivo y políticas de auditoría para archivos y carpetas con un estilo de seguridad NTFS efectivo en el volumen o qtree mixtos
- Protección del acceso a nivel de almacenamiento para volúmenes con seguridad efectiva de NTFS y UNIX

Volúmenes de estilo de seguridad de UNIX

Los volúmenes y qtrees de estilo de seguridad de UNIX contienen archivos y carpetas que tienen una seguridad efectiva de UNIX (bits de modo o ACL de NFSv4.x). Debe tener en cuenta lo siguiente si desea utilizar `vserver security file-directory` la familia de comandos para implementar la seguridad en volúmenes de estilo de seguridad de UNIX:

- ``vserver security file-directory`` La familia de comandos no se puede utilizar para gestionar las políticas de auditoría y seguridad de archivos UNIX en volúmenes y qtrees de tipo de seguridad de UNIX.
- ``vserver security file-directory`` La familia de comandos se puede usar para configurar Storage-Level Access Guard en volúmenes de seguridad de UNIX, siempre y cuando la SVM con el volumen de destino contenga un servidor CIFS.

Información relacionada

- [Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos](#)
- [Crear descriptores de seguridad NTFS en servidores](#)

- [Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas](#)
- [Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard](#)

Comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Dado que puede aplicar y administrar la seguridad de archivos y carpetas localmente sin la participación de un cliente remoto, puede reducir significativamente el tiempo que tarda en establecer la seguridad masiva en un gran número de archivos o carpetas.

Puede beneficiarse del uso de la CLI para establecer la seguridad de archivos y carpetas en los siguientes casos de uso:

- Almacenamiento de ficheros en entornos empresariales de gran tamaño, como el almacenamiento de ficheros en directorios iniciales
- Migración de datos
- Cambio de dominio de Windows
- Estandarización de las políticas de auditoría y seguridad de archivos en sistemas de archivos NTFS

Conozca los límites al usar comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Debe estar al tanto de determinados límites cuando utilice la CLI para establecer la seguridad de archivos y carpetas.

- ``vserver security file-directory`` La familia de comandos no admite la configuración de ACL NFSv4.

Sólo puede aplicar descriptores de seguridad NTFS a archivos y carpetas NTFS.

Utilice descriptores de seguridad para aplicar la seguridad de archivos y carpetas SMB de ONTAP

Los descriptores de seguridad contienen las listas de control de acceso que determinan qué acciones puede realizar un usuario en archivos y carpetas, y qué se audita cuando un usuario accede a archivos y carpetas.

• Permisos

El propietario de un objeto permite o deniega los permisos y determina qué acciones puede realizar un objeto (usuarios, grupos u objetos de equipo) en archivos o carpetas especificados.

• Descriptores de seguridad

Los descriptores de seguridad son estructuras de datos que contienen información de seguridad que definen los permisos asociados a un archivo o carpeta.

• Listas de control de acceso (ACL)

Las listas de control de acceso son las listas contenidas en un descriptor de seguridad que contienen información sobre las acciones que los usuarios, grupos o objetos de equipo pueden realizar en el archivo o la carpeta a la que se aplica el descriptor de seguridad. El descriptor de seguridad puede contener los

siguientes dos tipos de ACL:

- Listas de control de acceso discrecional (DACL)
- Listas de control de acceso del sistema (SACL)

- **Listas de control de acceso discrecional (DACL)**

Las DACL contienen la lista de SIDS para los usuarios, grupos y objetos de equipo a los que se permite o deniega el acceso para realizar acciones en archivos o carpetas. Las DACL contienen entradas de control de acceso cero o más (ACE).

- **Listas de control de acceso al sistema (SACL)**

SACL contiene la lista de SID para los usuarios, grupos y objetos de equipo para los que se registran eventos de auditoría correctos o fallidos. Las SACL contienen entradas de control de acceso cero o más (ACE).

- **Entradas de control de acceso (ACE)**

Las ACE son entradas individuales en DACL o SACL:

- Una entrada de control de acceso DACL especifica los derechos de acceso que se permiten o deniegan para determinados usuarios, grupos o objetos de equipo.
- Una entrada de control de acceso SACL especifica los eventos de éxito o de error que se deben registrar al auditar acciones especificadas realizadas por usuarios, grupos o objetos de equipo específicos.

- **Herencia de permisos**

La herencia de permisos describe cómo los permisos definidos en los descriptores de seguridad se propagan a un objeto de un objeto primario. Sólo los objetos secundarios heredan los permisos heredables. Al establecer permisos en el objeto padre, puede decidir si las carpetas, subcarpetas y archivos pueden heredarlos con «Aplicar a `this-folder, sub-folders y archivos`».

Información relacionada

- ["Seguimiento de seguridad y auditoría de SMB y NFS"](#)
- [Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas](#)

Obtenga información sobre cómo aplicar políticas de directorio de archivos que utilizan usuarios o grupos SMB locales en el destino de recuperación ante desastres de ONTAP SVM

Hay ciertas directrices que debe tener en cuenta antes de aplicar políticas de directorio de archivos en el destino de recuperación ante desastres de la máquina virtual de almacenamiento (SVM) en una configuración de descarte de ID si la configuración de la política de directorio de archivos usa usuarios o grupos locales en el descriptor de seguridad, o en las entradas DACL o SACL.

Puede configurar una configuración de recuperación ante desastres para una SVM donde la SVM de origen en el clúster de origen replica los datos y la configuración desde la SVM de origen a una SVM de destino en un clúster de destino.

Puede configurar uno de los dos tipos de recuperación ante desastres de SVM:

- Se conserva la identidad

Con esta configuración se conserva la identidad de la SVM y el servidor CIFS.

- Identidad descartada

Con esta configuración, no se conserva la identidad de la SVM y el servidor CIFS. En esta situación, el nombre de la SVM y el servidor CIFS en la SVM de destino es diferente de la SVM y del nombre del servidor CIFS en la SVM de origen.

Directrices para configuraciones de identidad descartadas

En una configuración de identidad descartada, en el caso de un origen de SVM que contenga configuraciones de usuarios locales, grupos y privilegios, se debe cambiar el nombre del dominio local (nombre del servidor CIFS local) para que coincida con el nombre del servidor CIFS en el destino de SVM. Por ejemplo, si el nombre de la SVM de origen es «vs1» y el nombre del servidor CIFS es «CIFS1» y el nombre de la SVM de destino es «vs1_dst» y el nombre del servidor CIFS es «CIFS1_DST», el nombre de dominio local de un usuario local denominado «CIFS1\user1» se cambia automáticamente a «CIFS1» en el destino».

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
administrator account			
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
administrator account			
vs1_dst	CIFS1_DST\user1	-	-

Aunque los nombres de usuario local y de grupos se modifican automáticamente en las bases de datos de usuario local y de grupos, los usuarios locales o los nombres de grupo no se modifican automáticamente en las configuraciones de las políticas de directorio de archivos (las políticas configuradas en la interfaz de línea de `vserver security file-directory` comandos mediante la familia de comandos).

Por ejemplo, para «VS1», si ha configurado una entrada DACL en la que el `-account` parámetro se establece en «CIFS1\user1», la configuración no se cambia automáticamente en la SVM de destino para reflejar el nombre del servidor CIFS del destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sdl
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sdl
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

Debe utilizar `vserver security file-directory modify` los comandos para cambiar manualmente el nombre del servidor CIFS al nombre del servidor CIFS de destino.

Componentes de configuración de directivas de directorio de archivos que contienen parámetros de cuenta

Existen tres componentes de configuración de directivas de directorio de archivos que pueden utilizar parámetros que pueden contener usuarios o grupos locales:

- Descriptor de seguridad

Opcionalmente, puede especificar el propietario del descriptor de seguridad y el grupo primario del propietario del descriptor de seguridad. Si el descriptor de seguridad utiliza un usuario o grupo local para las entradas del propietario y del grupo primario, debe modificar el descriptor de seguridad para utilizar la SVM de destino en el nombre de cuenta. Puede usar el `vserver security file-directory ntfs modify` comando para realizar los cambios necesarios en los nombres de cuentas.

- Entradas de DACL

Cada entrada de DACL debe estar asociada a una cuenta. Debe modificar todas las DACL que utilicen cuentas de usuario local o de grupo para usar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas DACL existentes, debe eliminar todas las entradas DACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas DACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas DACL con los descriptores de seguridad adecuados.

- Entradas de SACL

Cada entrada de SACL debe estar asociada a una cuenta. Debe modificar todas las SACL que utilicen

cuentas de usuario o de grupo local para utilizar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas SACL existentes, debe eliminar todas las entradas SACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas SACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas SACL con los descriptores de seguridad adecuados.

Debe realizar los cambios necesarios en los usuarios o grupos locales utilizados en la configuración de la directiva de directorio de archivos antes de aplicar la directiva; de lo contrario, el trabajo de aplicación fallará.

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear un descriptor de seguridad NTFS (política de seguridad de archivos) es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en máquinas virtuales de almacenamiento (SVM). Puede asociar el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más

información en el ["Referencia de comandos del ONTAP"](#).

Agregue entradas de control de acceso NTFS DACL a los descriptores de seguridad NTFS en servidores SMB de ONTAP

La adición de entradas de control de acceso (ACE) de DACL (lista de control de acceso discrecional) al descriptor de seguridad de NTFS es el segundo paso para configurar y aplicar ACL de NTFS a un archivo o carpeta. Cada entrada identifica qué objeto tiene permiso o acceso denegado, y define lo que el objeto puede o no puede hacer con los archivos o carpetas definidos en ACE.

Acerca de esta tarea

Puede añadir una o varias ACE a la DACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una DACL que tiene ACE existentes, el comando agrega la nueva ACE a la DACL. Si el descriptor de seguridad no contiene una DACL, el comando crea la DACL y le agrega la nueva ACE.

Opcionalmente, puede personalizar las entradas DACL especificando qué derechos desea permitir o denegar para la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)



Si no especifica derechos para la entrada DACL, el valor predeterminado es establecer los derechos en Full Control.

Opcionalmente, puede personalizar las entradas DACL especificando cómo aplicar herencia.

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Agregue una entrada DACL a un descriptor de seguridad: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID optional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Compruebe que la entrada DACL es correcta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```

Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
      Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
    Access Rights: full-control

```

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el ["Referencia de comandos del ONTAP"](#).

Crear políticas de seguridad de ONTAP SMB

Crear una política de seguridad de archivos para SVM es el tercer paso a la hora de configurar y aplicar ACL a un archivo o carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada SVM (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```

vserver security file-directory policy show
Vserver          Policy Name
-----
vs1              policy1

```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

Nunca dará permisos de acceso adicionales.

Al agregar tareas a las directivas de seguridad, debe especificar los siguientes cuatro parámetros necesarios:

- Nombre de SVM
- Nombre de la política
- Ruta
- Descriptor de seguridad que se asociará a la ruta de acceso

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice

- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	

1	/home/dir1	file-directory	ntfs	propagate	sd2

Obtenga más información sobre `vserver security file-directory policy task` en el ["Referencia de comandos del ONTAP"](#).

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de seguridad de archivos a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).



Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job	ID	Name	Vserver	Node	State
53322		Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job					

Verificar la seguridad de los archivos SMB de ONTAP

Es posible verificar la configuración de seguridad de archivos para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración deseada.

Acerca de esta tarea

Debe suministrar el nombre de la SVM que contenga los datos y la ruta de acceso al archivo y las carpetas en los que desea verificar la configuración de seguridad. Puede utilizar el parámetro opcional `-expand-mask` para mostrar información detallada sobre la configuración de seguridad.

Paso

1. Mostrar configuración de seguridad de archivos y carpetas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
Vserver: vs1
      File Path: /data/engineering
File Inode Number: 5544
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8004

1... .... = Self Relative
.0.. .... = RM Control Valid
..0. .... = SACL Protected
...0 .... = DACL Protected
.... 0... = SACL Inherited
.... .0.. = DACL Inherited
.... ..0. = SACL Inherit Required
.... ...0 = DACL Inherit Required
.... .... ..0. = SACL Defaulted
.... .... ...0 = SACL Present
.... .... .... 0... = DACL Defaulted
.... .... .... .1.. = DACL Present
```

```

      ....  ....  ....  ..0. = Group Defaulted
      ....  ....  ....  ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
      ALLOW-Everyone-0x1f01ff
      0...  ....  ....  ....  ....  ....  ....  ....  ....  ....  =
Generic Read
      .0..  ....  ....  ....  ....  ....  ....  ....  ....  ....  =
Generic Write
      ..0.  ....  ....  ....  ....  ....  ....  ....  ....  ....  =
Generic Execute
      ...0  ....  ....  ....  ....  ....  ....  ....  ....  ....  =
Generic All
      ....  ...0  ....  ....  ....  ....  ....  ....  ....  ....  =
System Security
      ....  ....  ...1  ....  ....  ....  ....  ....  ....  ....  =
Synchronize
      ....  ....  ....  1...  ....  ....  ....  ....  ....  ....  =
Write Owner
      ....  ....  ....  .1..  ....  ....  ....  ....  ....  ....  =
Write DAC
      ....  ....  ....  ..1.  ....  ....  ....  ....  ....  ....  =
Read Control
      ....  ....  ....  ...1  ....  ....  ....  ....  ....  ....  =
Delete
      ....  ....  ....  ....  ....  ....  ...1  ....  ....  ....  =
Write Attributes
      ....  ....  ....  ....  ....  ....  ....  1...  ....  ....  =
Read Attributes
      ....  ....  ....  ....  ....  ....  ....  .1..  ....  ....  =
Delete Child
      ....  ....  ....  ....  ....  ....  ....  ..1.  ....  ....  =
Execute
      ....  ....  ....  ....  ....  ....  ....  ...1  ....  ....  =
Write EA
      ....  ....  ....  ....  ....  ....  ....  ....  1...  ....  =
Read EA
      ....  ....  ....  ....  ....  ....  ....  ....  .1..  ....  =
Append
      ....  ....  ....  ....  ....  ....  ....  ....  ..1.  ....  =
Write
      ....  ....  ....  ....  ....  ....  ....  ....  ...1  ....  =
Read

```

	ALLOW-Everyone-0x10000000-OI CI IO	
	0... .. =	
Generic Read		
	.0.. .. =	
Generic Write		
	..0. =	
Generic Execute		
	...1 =	
Generic All		
	0 =	
System Security		
	0 =	
Synchronize		
	 0... .. =	
Write Owner		
	0.. .. =	
Write DAC		
	0. =	
Read Control		
	0 =	
Delete		
	 0 =	
Write Attributes		
	 0... .. =	
Read Attributes		
	0.. .. =	
Delete Child		
	0. =	
Execute		
	0 =	
Write EA		
	 0... =	
Read EA		
	0.. =	
Append		
	0. =	
Write		
	0 =	
Read		

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos

Comandos ONTAP para configurar y aplicar políticas de auditoría SMB a archivos y carpetas NTFS

Hay varios pasos que debe realizar para aplicar políticas de auditoría a archivos y carpetas NTFS cuando use la CLI de ONTAP. En primer lugar, debe crear un descriptor de seguridad NTFS y agregar SACL al descriptor de seguridad. A continuación, cree una directiva de seguridad y agregue tareas de directiva. Luego, debe aplicar la política de seguridad a una SVM.

Acerca de esta tarea

Después de aplicar la directiva de seguridad, puede supervisar el trabajo de directiva de seguridad y, a continuación, verificar la configuración de la directiva de auditoría aplicada.



Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Información relacionada

- [Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard](#)
- [Conozca los límites al usar comandos para configurar la seguridad de archivos y carpetas SMB](#)
- [Utilice descriptores de seguridad para aplicar seguridad a archivos y carpetas](#)
- ["Seguimiento de seguridad y auditoría de SMB y NFS"](#)
- [Crear descriptores de seguridad NTFS en servidores](#)

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear una política de auditoría de descriptor de seguridad NTFS es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en SVM. Asociará el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Si desea utilizar los parámetros avanzados, configure el nivel de privilegio en advanced: `set -privilege advanced`
2. Cree un descriptor de seguridad: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. Compruebe que la configuración del descriptor de seguridad es correcta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Si se encuentra en el nivel de privilegio avanzado, vuelva al nivel de privilegio de administrador: `set -privilege admin`

Agregue entradas de control de acceso SACL NTFS a los descriptors de seguridad NTFS en servidores SMB de ONTAP

Añadir entradas de control de acceso (ACE) SACL (lista de control de acceso del sistema) al descriptor de seguridad NTFS es el segundo paso a la hora de crear directivas de auditoría NTFS para archivos o carpetas en SVM. Cada entrada identifica el

usuario o grupo que desea auditar. La entrada SACL define si desea auditar los intentos de acceso fallidos o correctos.

Acerca de esta tarea

Puede añadir una o varias ACE a la SACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una SACL que tiene ACE existentes, el comando agrega la nueva ACE a la SACL. Si el descriptor de seguridad no contiene una SACL, el comando crea la SACL y le agrega la nueva ACE.

Puede configurar entradas de SACL especificando los derechos que desea auditar para eventos de éxito o fallo de la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)



Si no especifica derechos para la entrada SACL, el valor por defecto es `Full Control`.

Opcionalmente, puede personalizar las entradas de SACL especificando cómo aplicar la herencia con el `apply to` parámetro. Si no especifica este parámetro, el valor predeterminado es aplicar esta entrada SACL a esta carpeta, subcarpetas y archivos.

Pasos

1. Agregue una entrada SACL a un descriptor de seguridad: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID optional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Compruebe que la entrada de SACL es correcta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

Crear políticas de seguridad de ONTAP SMB

Crear una política de auditoría para máquinas virtuales de almacenamiento (SVM) es el tercer paso a la hora de configurar y aplicar ACL a un archivo o una carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada máquina virtual de almacenamiento (SVM) (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
      Vserver          Policy Name
      -----          -
      vs1              policy1
```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

Nunca dará permisos de acceso adicionales.

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	

1	/home/dir1	file-directory	ntfs	propagate	sd2

Obtenga más información sobre `vserver security file-directory policy task` en el ["Referencia de comandos del ONTAP"](#).

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de auditoría a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).



Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que

está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

Verificar las políticas de auditoría de ONTAP SMB

Puede verificar la política de auditoría para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración de seguridad de auditoría deseada.

Acerca de esta tarea

El `vserver security file-directory show` comando se utiliza para mostrar información sobre la política de auditoría. Debe proporcionar el nombre de la SVM que contiene los datos y la ruta a los datos cuyo archivo o carpeta de información de la política de auditoría que desea mostrar.

Paso

1. Mostrar configuración de política de auditoría: `vserver security file-directory show -vserver vserver_name -path path`

Ejemplo

El siguiente comando muestra la información de la directiva de auditoría aplicada a la ruta `"/corp"` en SVM `vs1`. La ruta de acceso tiene aplicada UNA entrada SACL DE ÉXITO y DE FALLO:

```

cluster::> vsriver security file-directory show -vsriver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

Obtenga información sobre cómo administrar los trabajos de políticas de seguridad de ONTAP SMB

Si existe un trabajo de política de seguridad, en determinadas circunstancias, no puede modificar dicha política de seguridad ni las tareas asignadas a dicha política. Debe entender en qué condiciones puede o no puede modificar las directivas de seguridad para que cualquier intento que realice para modificar la directiva se realice correctamente. Las modificaciones de la directiva incluyen agregar, eliminar o modificar tareas asignadas a la directiva y eliminar o modificar la directiva.

No puede modificar una política de seguridad ni una tarea asignada a esa política si existe un trabajo para esa política y ese trabajo está en los estados siguientes:

- El trabajo está en ejecución o en curso.
- El trabajo está en pausa.
- El trabajo se reanuda y se encuentra en estado en ejecución.
- Si el trabajo está esperando a conmutar al respaldo a otro nodo.

En las siguientes circunstancias, si existe un trabajo para una política de seguridad, puede modificar

correctamente dicha política de seguridad o una tarea asignada a dicha directiva:

- El trabajo de política se ha detenido.
- El trabajo de directiva ha finalizado correctamente.

Comandos ONTAP para administrar descriptores de seguridad NTFS en servidores SMB

Existen comandos ONTAP específicos para administrar descriptores de seguridad. Puede crear, modificar, eliminar y mostrar información acerca de los descriptores de seguridad.

Si desea...	Se usa este comando...
Crear descriptores de seguridad NTFS	<code>vserver security file-directory ntfs create</code>
Modifique los descriptores de seguridad NTFS existentes	<code>vserver security file-directory ntfs modify</code>
Mostrar información acerca de los descriptores de seguridad NTFS existentes	<code>vserver security file-directory ntfs show</code>
Eliminar descriptores de seguridad NTFS	<code>vserver security file-directory ntfs delete</code>

Obtenga más información sobre `vserver security file-directory ntfs` en el ["Referencia de comandos del ONTAP"](#).

Comandos ONTAP para administrar entradas de control de acceso DACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso DACL (ACE). Puede agregar ACE a DACL NTFS en cualquier momento. También puede administrar las DACL de NTFS existentes modificando, eliminando y mostrando información acerca de las ACE en las DACL.

Si desea...	Se usa este comando...
Cree ACE y agréguelos a DACL NTFS	<code>vserver security file-directory ntfs dacl add</code>
Modifique los ACE existentes en las DACL NTFS	<code>vserver security file-directory ntfs dacl modify</code>
Mostrar información acerca de los ACE existentes en las DACL NTFS	<code>vserver security file-directory ntfs dacl show</code>

Si desea...	Se usa este comando...
Elimine los ACE existentes de las DACL NTFS	<code>vserver security file-directory ntfs dacl remove</code>

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el ["Referencia de comandos del ONTAP"](#).

Comandos ONTAP para administrar entradas de control de acceso SACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso SACL (ACE). Puede agregar ACE a SACL NTFS en cualquier momento. También puede administrar SACL NTFS existentes modificando, eliminando y mostrando información acerca de ACE en SACL.

Si desea...	Se usa este comando...
Cree ACE y agréguelos a SACL NTFS	<code>vserver security file-directory ntfs sac1 add</code>
Modifique los ACE existentes en SACL NTFS	<code>vserver security file-directory ntfs sac1 modify</code>
Muestra información acerca de los ACE existentes en SACL NTFS	<code>vserver security file-directory ntfs sac1 show</code>
Elimine los ACE existentes de SACL NTFS	<code>vserver security file-directory ntfs sac1 remove</code>

Obtenga más información sobre `vserver security file-directory ntfs sac1` en el ["Referencia de comandos del ONTAP"](#).

Comandos de ONTAP para administrar políticas de seguridad SMB

Existen comandos ONTAP específicos para administrar las políticas de seguridad. Puede mostrar información acerca de las políticas y eliminarla. No puede modificar una política de seguridad.

Si desea...	Se usa este comando...
Cree políticas de seguridad	<code>vserver security file-directory policy create</code>
Mostrar información acerca de las directivas de seguridad	<code>vserver security file-directory policy show</code>

Si desea...	Se usa este comando...
Eliminar políticas de seguridad	<code>vserver security file-directory policy delete</code>

Obtenga más información sobre `vserver security file-directory policy` en el ["Referencia de comandos del ONTAP"](#).

Comandos ONTAP para administrar tareas de políticas de seguridad SMB

Hay comandos de ONTAP para añadir, modificar, quitar y mostrar información acerca de tareas de políticas de seguridad.

Si desea...	Se usa este comando...
Agregar tareas de directiva de seguridad	<code>vserver security file-directory policy task add</code>
Modifique las tareas de las políticas de seguridad	<code>vserver security file-directory policy task modify</code>
Muestra información acerca de las tareas de directiva de seguridad	<code>vserver security file-directory policy task show</code>
Quitar tareas de directiva de seguridad	<code>vserver security file-directory policy task remove</code>

Obtenga más información sobre `vserver security file-directory policy task` en el ["Referencia de comandos del ONTAP"](#).

Comandos de ONTAP para administrar trabajos de políticas de seguridad de SMB

Hay comandos de la ONTAP para pausar, reanudar, detener y mostrar información acerca de los trabajos de políticas de seguridad.

Si desea...	Se usa este comando...
Pausar trabajos de directiva de seguridad	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
Reanudar trabajos de directiva de seguridad	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
Mostrar información sobre trabajos de directivas de seguridad	<code>vserver security file-directory job show -vserver vserver_name</code> Puede determinar el ID de trabajo de un trabajo mediante este comando.

Si desea...	Se usa este comando...
Detener trabajos de directiva de seguridad	<pre>vserver security file-directory job stop -vserver vserver_name -id integer</pre>

Obtenga más información sobre `vserver security file-directory job` en el ["Referencia de comandos del ONTAP"](#).

Configure la caché de metadatos para los recursos compartidos de SMB

Obtenga más información sobre el almacenamiento en caché de metadatos SMB de ONTAP

El almacenamiento en caché de metadatos permite almacenar en caché atributos de archivos en clientes SMB 1.0 para proporcionar un acceso más rápido a los atributos de archivos y carpetas. Puede habilitar o deshabilitar el almacenamiento en caché de atributos por recurso compartido. También puede configurar el tiempo de espera para las entradas en caché si está activado el almacenamiento en caché de metadatos. No es necesario configurar el almacenamiento en caché de metadatos si los clientes se conectan a recursos compartidos mediante SMB 2.x o SMB 3.0.

Cuando se habilita esta opción, la caché de metadatos del SMB almacena los datos de atributos de archivos y rutas por una cantidad limitada de tiempo. Esto puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 con cargas de trabajo comunes.

En determinadas tareas, SMB crea una cantidad significativa de tráfico que puede incluir varias consultas idénticas para los metadatos de archivos y rutas. Puede reducir el número de consultas redundantes y mejorar el rendimiento de clientes de SMB 1.0 utilizando el almacenamiento en caché de metadatos del SMB para recuperar información de la caché.



Si bien es poco probable, es posible que la caché de metadatos proporcione información obsoleta a clientes SMB 1.0. Si su entorno no se puede permitir este riesgo, no debe habilitar esta función.

Habilitar la caché de metadatos SMB de ONTAP

Puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 al habilitar la caché de metadatos de SMB. De manera predeterminada, el almacenamiento en caché de metadatos de SMB está deshabilitado.

Paso

1. Realice la acción deseada:

Si desea...	Introduzca el comando...
Habilite el almacenamiento en caché de metadatos de SMB cuando crea un recurso compartido	<code>vserver cifs share create -vserver <i>vserver_name</i> -share-name <i>share_name</i> -path <i>path</i> -share-properties attributecache</code>
Habilite el almacenamiento en caché de metadatos de SMB en un recurso compartido existente	<code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties attributecache</code>

Información relacionada

- [Configurar la duración de las entradas de caché de metadatos](#)
- [Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes](#)

Configurar la duración de las entradas de caché de metadatos SMB de ONTAP

Puede configurar la vida útil de las entradas de la caché de metadatos SMB para optimizar el rendimiento de la caché de metadatos de SMB en su entorno. El valor predeterminado es 10 segundos.

Antes de empezar

Debe haber habilitado la función de caché de metadatos SMB. Si el almacenamiento en caché de metadatos de SMB no está habilitado, no se utiliza la configuración TTL de la caché de SMB.

Paso

1. Realice la acción deseada:

Si desea configurar la vida útil de las entradas de la caché de metadatos SMB al...	Introduzca el comando...
Crear un recurso compartido	<code>vserver cifs share -create -vserver <i>vserver_name</i> -share-name <i>share_name</i> -path <i>path</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>
Modifique un recurso compartido existente	<code>vserver cifs share -modify -vserver <i>vserver_name</i> -share-name <i>share_name</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>

Puede especificar propiedades y opciones de configuración de recursos compartidos adicionales al crear o modificar recursos compartidos. Obtenga más información sobre `vserver cifs share` en el ["Referencia de comandos del ONTAP"](#).

Administrar bloqueos de archivos

Obtenga información sobre el bloqueo de archivos SMB de ONTAP entre protocolos

El bloqueo de archivos es un método que utilizan las aplicaciones cliente para evitar que un usuario acceda a un archivo abierto previamente por otro usuario. La forma en que ONTAP bloquea los archivos depende del protocolo del cliente.

Si el cliente es NFS, los bloqueos son consultivos; si el cliente es un cliente SMB, los bloqueos son obligatorios.

Debido a las diferencias entre los bloqueos de archivos NFS y SMB, es posible que un cliente NFS no pueda acceder a un archivo que abrió previamente una aplicación SMB.

Lo siguiente se produce cuando un cliente NFS intenta acceder a un archivo bloqueado por una aplicación SMB:

- En volúmenes mixtos o NTFS, las operaciones de manipulación de archivos `rm` como `rm`, `rmdir` y `mv` pueden provocar el fallo de la aplicación NFS.
- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos `Deny-Read` y `Deny-write` de SMB, respectivamente.
- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un `bytelock` exclusivo de SMB.
- Desenlazar
 - En el caso de los sistemas de archivos NTFS, se admiten las operaciones de eliminación de SMB y CIFS.

El archivo se eliminará después del último cierre.

- No se admiten las operaciones de desenlace de NFS.

No es compatible porque la semántica NTFS y SMB es necesaria, y la última operación `Delete-on-Close` no es compatible con NFS.

- Para los sistemas de archivos UNIX, se admite la operación de desvinculación.

Es compatible porque se necesitan semántica NFS y UNIX.

- Cambiar el nombre
 - Para los sistemas de archivos NTFS, si el archivo de destino se abre desde SMB o CIFS, se puede cambiar el nombre del archivo de destino.
 - No se admite el cambio de nombre de NFS.

No es compatible porque se requieren semánticas NTFS y SMB.

En los volúmenes de estilo de seguridad de UNIX, las operaciones de desenlace y cambio de nombre de NFS ignoran el estado de bloqueo de SMB y permiten el acceso al archivo. Todas las demás operaciones de NFS en volúmenes de estilo de seguridad de UNIX honran el estado de bloqueo de SMB.

Obtenga información sobre los bits de solo lectura de ONTAP SMB

El bit de sólo lectura se establece en base a archivo para reflejar si un archivo es grabable (deshabilitado) o de sólo lectura (habilitado).

Los clientes SMB que usan Windows pueden establecer un bit de solo lectura por archivo. Los clientes NFS no establecen un bit de solo lectura por archivo, ya que los clientes NFS no tienen ninguna operación de protocolo que utilice un bit de solo lectura por archivo.

ONTAP puede establecer un bit de solo lectura en un archivo cuando un cliente SMB que utiliza Windows crea ese archivo. ONTAP también puede establecer un bit de solo lectura cuando se comparte un archivo entre los clientes NFS y los clientes SMB. Parte del software, cuando lo utilizan los clientes NFS y clientes SMB, requiere que se habilite el bit de solo lectura.

Para que ONTAP mantenga los permisos de lectura y escritura adecuados en un archivo compartido entre clientes NFS y clientes SMB, trata el bit de solo lectura de acuerdo con las siguientes reglas:

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.
- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para ese archivo.
- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.

El bit de solo lectura interactúa con los bits de modo ACL y Unix de las siguientes maneras:

Cuando el bit de solo lectura está configurado en un archivo:

- No se realizan cambios en la ACL de ese archivo. Los clientes NFS verán la misma ACL que antes de configurar el bit de solo lectura.
- Se ignoran todos los bits del modo Unix que permiten acceso de escritura al archivo.
- Tanto los clientes NFS como SMB pueden leer el archivo, pero no pueden modificarlo.
- Las ACL y los bits de modo UNIX se ignoran en favor del bit de solo lectura. Esto significa que, incluso si la ACL permite el acceso de escritura, el bit de solo lectura impide las modificaciones.

Cuando el bit de solo lectura no está configurado en un archivo:

- ONTAP determina el acceso según los bits de modo ACL y UNIX.
 - Si los bits del modo ACL o UNIX niegan el acceso de escritura, los clientes NFS y SMB no pueden modificar el archivo.
 - Si ni los bits del modo ACL ni los del modo UNIX niegan el acceso de escritura, los clientes NFS y SMB pueden modificar el archivo.



Los cambios en los permisos de archivo se aplican inmediatamente en los clientes SMB, pero es posible que no se apliquen de inmediato en los clientes NFS si el cliente NFS habilita el almacenamiento de atributos en caché.

Diferencias entre ONTAP y Windows en el manejo de bloqueos en componentes de ruta de acceso compartida

A diferencia de Windows, ONTAP no bloquea cada componente de la ruta de acceso a un archivo abierto mientras el archivo está abierto. Este comportamiento también afecta a las rutas de recursos compartidos de SMB.

Como ONTAP no bloquea cada componente de la ruta, es posible cambiar el nombre de un componente de ruta por encima del archivo o el recurso compartido abierto, lo que puede provocar problemas en determinadas aplicaciones o hacer que la ruta del recurso compartido en la configuración del SMB no sea válida. Esto puede hacer que el recurso compartido sea inaccesible.

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede aplicar configuraciones de seguridad que impidan que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Mostrar información sobre los bloqueos SMB de ONTAP

Puede mostrar información acerca de los bloqueos de archivos actuales, incluidos los tipos de bloqueos que se conservan y el estado de bloqueo, detalles sobre bloqueos de rango de bytes, modos sharelock, bloqueos de delegación y bloqueos oportunistas, y si se abren bloqueos con identificadores duraderos o persistentes.

Acerca de esta tarea

No se puede mostrar la dirección IP del cliente para los bloqueos establecidos a través de NFSv4 o NFSv4.1.

De forma predeterminada, el comando muestra información sobre todos los bloqueos. Puede usar los parámetros del comando para mostrar información sobre los bloqueos de una máquina virtual de almacenamiento (SVM) específica o para filtrar el resultado del comando según otros criterios.

El `vserver locks show` comando muestra información sobre cuatro tipos de bloqueos:

- Bloqueos de rango de bytes, que bloquean sólo una parte de un archivo.
- Bloqueos de uso compartido, que bloquean los archivos abiertos.
- Bloqueos oportunistas, que controlan el almacenamiento en caché en el cliente a través de SMB.
- Delegaciones, que controlan el almacenamiento en caché en el cliente a través de NFSv4.x.

Al especificar parámetros opcionales, puede determinar información importante sobre cada tipo de bloqueo. Obtenga más información sobre `vserver locks show` en el ["Referencia de comandos del ONTAP"](#).

Paso

1. Muestra información sobre los bloqueos mediante `vserver locks show` el comando.

Ejemplos

El siguiente ejemplo muestra información de resumen para un bloqueo NFSv4 en un archivo con la ruta

/vol1/file1. El modo de acceso sharelock es write-deny_none, y el bloqueo se concedió mediante la delegación de escritura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1               lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

El siguiente ejemplo muestra información detallada sobre el bloqueo operativo y el bloqueo compartido sobre el bloqueo SMB en un archivo con la ruta de acceso /data2/data2_2/intro.pptx. Se concede un identificador duradero en el archivo con un modo de acceso de bloqueo compartido de Write-Deny_none a un cliente con una dirección IP de 10.3.1.3. Un plock de arrendamiento se concede con un nivel de plock por lotes:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: -
Shared Lock Access Mode: write-deny_none
Shared Lock is Soft: false
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: durable
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
```

```

78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/test.pptx
Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
Lock Protocol: cifs
Lock Type: op-lock
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

Romper los bloqueos SMB de ONTAP

Cuando los bloqueos de archivos impiden que los clientes accedan a los archivos, puede mostrar información sobre los bloqueos retenidos actualmente y romperán bloqueos específicos. Entre los ejemplos de escenarios en los que es posible que necesite romper los bloqueos se incluyen las aplicaciones de depuración.

Acerca de esta tarea

```

`vserver locks break`El comando solo está disponible en el nivel de
privilegios avanzado y superior. Obtenga más información sobre `vserver
locks break` en el link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["Referencia de comandos del ONTAP"^].

```

Pasos

1. Para encontrar la información que necesita para romper un bloqueo, utilice el `vserver locks show` comando.

Obtenga más información sobre `vserver locks show` en el ["Referencia de comandos del ONTAP"](#).

2. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
3. Ejecute una de las siguientes acciones:

Si desea romper un bloqueo especificando...	Introduzca el comando...
El nombre de SVM, el nombre del volumen, el nombre de LIF y la ruta de archivo	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
El ID del bloqueo	<code>vserver locks break -lockid UUID</code>

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

Supervise la actividad del SMB

Mostrar información de la sesión SMB de ONTAP

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede utilizar el parámetro opcional `-fields` para mostrar resultados sobre los campos seleccionados.

Puede introducir `-fields ?` para determinar qué campos puede utilizar.

- Puede usar el `-instance` parámetro para mostrar información detallada acerca de las sesiones SMB establecidas.
- Puede usar `-fields` el parámetro o el `-instance` parámetro solo o en combinación con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información de la sesión SMB...	Introduzca el siguiente comando...
Para todas las sesiones del SVM en formato de resumen	<code>vserver cifs session show -vserver vserver_name</code>
En un ID de conexión especificado	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
Desde una dirección IP de estación de trabajo especificada	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
En una dirección IP de LIF especificada	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
En un nodo especificado	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
local}`	Desde un usuario de Windows especificado
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	Con un mecanismo de autenticación especificado
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
Con una versión de protocolo especificada	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1
SMB3	SMB3_1}`
	[NOTE] ==== Protección de disponibilidad continua y multicanal de SMB solo están disponibles en sesiones SMB 3.0 y posteriores. Para ver su estado en todas las sesiones de calificación, debe especificar este parámetro con el valor definido en SMB3 o posterior. ====
Con un nivel especificado de protección continua disponible	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>

Si desea mostrar información de la sesión SMB...	Introduzca el siguiente comando...
Yes	Partial}` [NOTE] ==== Si el estado de disponibilidad continua es <code>Partial</code> , significa que la sesión contiene al menos un archivo abierto continuamente disponible, pero la sesión tiene algunos archivos que no están abiertos con protección disponible continuamente. Puede usar el <code>vserver cifs sessions file show</code> comando para determinar qué archivos de la sesión establecida no están abiertos con la protección disponible continuamente. ====
Con un estado de sesión de firma SMB especificado	<code>`vserver cifs session show -vserver vserver_name -is-session-signed {true</code>

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation    Windows User    Open    Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1      DOMAIN\joe      2       23s
```

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
Node: node1  
Vserver: vs1  
Session ID: 1  
Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
Windows User: DOMAIN\SERVER1$  
UNIX User: pcuser  
Open Shares: 1  
Open Files: 1  
Open Other: 0  
Connected Time: 10m 43s  
Idle Time: 1m 19s  
Protocol Version: SMB3  
Continuously Available: Yes  
Is Session Signed: false  
User Authenticated as: domain-user  
NetBIOS Name: -  
SMB Encryption Status: Unencrypted
```

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```

    Node: node1
    Vserver: vs1
    Session ID: 1
    **Connection IDs: 3151272607,31512726078,3151272609
    Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
    Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
        Windows User: DOMAIN\administrator
        UNIX User: pcuser
    Open Shares: 1
    Open Files: 0
    Open Other: 0
    Connected Time: 6m 22s
    Idle Time: 5m 42s
    Protocol Version: SMB3
    Continuously Available: No
    Is Session Signed: false
    User Authenticated as: domain-user
    NetBIOS Name: -
    SMB Encryption Status: Unencrypted
```

Información relacionada

[Mostrar información acerca de los archivos SMB abiertos](#)

Mostrar información sobre archivos SMB de ONTAP abiertos

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. Es posible mostrar información acerca del nivel de protección disponible continuamente de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos de los archivos abiertos están abiertos con protección disponible continuamente y otros no están abiertos con protección disponible continuamente (el valor `-continuously-available` del campo en `vserver cifs session show` la salida del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida, mediante `vserver cifs session file show` el

comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede utilizar el parámetro opcional `-fields` para mostrar la salida en los campos seleccionados.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

- Puede utilizar el `-instance` parámetro para mostrar información detallada sobre los archivos SMB abiertos.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar archivos SMB abiertos...	Introduzca el siguiente comando...
En la SVM de forma resumida	<pre>vserver cifs session file show -vserver vserver_name</pre>
En un nodo especificado	<pre>`vserver cifs session file show -vserver vserver_name -node {node_name</pre>
local}`	En un ID de archivo especificado
<pre>vserver cifs session file show -vserver vserver_name -file-id integer</pre>	En un ID de conexión de SMB especificado
<pre>vserver cifs session file show -vserver vserver_name -connection-id integer</pre>	En un ID de sesión de SMB especificado
<pre>vserver cifs session file show -vserver vserver_name -session-id integer</pre>	En el agregado de host especificado
<pre>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</pre>	En el volumen especificado
<pre>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</pre>	En el recurso compartido de SMB especificado

Si desea mostrar archivos SMB abiertos...	Introduzca el siguiente comando...
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	En la ruta del bloque de mensajes del servidor especificada
<code>vserver cifs session file show -vserver vserver_name -path path</code>	Con el nivel especificado de protección continua disponible
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes} [NOTE] ==== Si el estado de disponibilidad continua es No, esto significa que estos archivos abiertos no pueden recuperarse sin interrupciones de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad. ====
Con el estado reconectado especificado	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Obtenga más información sobre `vserver cifs session file show` en el ["Referencia de comandos del ONTAP"](#).

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID        Type       Mode Volume      Share      Available
-----
41        Regular    r    data      data      Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```

        Node: node1
        Vserver: vs1
        File ID: 82
    Connection ID: 104617
        Session ID: 1
        File Type: Regular
        Open Mode: rw
Aggregate Hosting File: aggr1
    Volume Hosting File: data1
        CIFS Share: data1
    Path from CIFS Share: windows\win8\test\test.txt
        Share Mode: rw
        Range Locks: 1
Continuously Available: Yes
        Reconnected: No
```

Información relacionada

[Mostrar información de la sesión](#)

Determinar qué estadísticas, objetos y contadores están disponibles en los servidores SMB de ONTAP

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea determinar...	Introduzca...
Qué objetos están disponibles	<code>statistics catalog object show</code>
Objetos específicos disponibles	<code>statistics catalog object show -object object_name</code>
Qué contadores están disponibles	<code>statistics catalog counter show -object object_name</code>

Obtenga más información sobre `statistics catalog object show`, incluidos los objetos y contadores disponibles, en la ["Referencia de comandos del ONTAP"](#) sección .

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                    The CIFS object reports activity of the
                           Common Internet File System protocol
                           ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs             The Common Internet File System (CIFS)
                           protocol is an implementation of the
Server
                           ...

cluster1::*> statistics catalog object show -object smb1
    smb1                   These counters report activity from the
SMB
                           revision of the protocol. For information
                           ...

cluster1::*> statistics catalog object show -object smb2
    smb2                   These counters report activity from the
                           SMB2/SMB3 revision of the protocol. For
                           ...

cluster1::*> statistics catalog object show -object hashd
    hashd                  The hashd object provides counters to
measure
                           the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos de los contadores del `cifs` objeto como se ve

en el nivel de privilegio avanzado:



En este ejemplo no se muestran todos los contadores disponibles para `cifs` el objeto; la salida se trunca.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

Información relacionada

- [Mostrar estadísticas](#)
- ["Catálogo de estadísticas Contador Mostrar objeto"](#)

- ["Las estadísticas comienzan"](#)

Mostrar estadísticas de ONTAP SMB

Puede mostrar varias estadísticas, incluidas estadísticas sobre CIFS y SMB, auditoría y hash de BranchCache, para supervisar el rendimiento y diagnosticar problemas.

Antes de empezar

Debe haber recogido muestras de datos mediante los `statistics start statistics stop` comandos y antes de poder mostrar información sobre los objetos.

Obtenga más información sobre `statistics start` y `statistics stop` en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea mostrar estadísticas de...	Introduzca...
Todas las versiones de SMB	<code>statistics show -object cifs</code>
SMB 1,0	<code>statistics show -object smb1</code>
SMB 2.x y SMB 3.0	<code>statistics show -object smb2</code>
Subsistema CIFS del nodo	<code>statistics show -object nblade_cifs</code>
Auditoría multiprotocolo	<code>statistics show -object audit_ng</code>
Servicio hash de BranchCache	<code>statistics show -object hashd</code>
DNS dinámico	<code>statistics show -object ddns_update</code>

Obtenga más información sobre `statistics show` en el ["Referencia de comandos del ONTAP"](#).

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

- [Determinar qué estadísticas, objetos y contadores están disponibles en los servidores](#)
- [Supervisar estadísticas de sesión firmada por SMB](#)
- [Muestra las estadísticas de BranchCache](#)
- [Utilice estadísticas para supervisar la actividad de referencia automática de nodos](#)
- ["Configuración de SMB para Microsoft Hyper-V y SQL Server"](#)
- ["Configuración de supervisión del rendimiento"](#)

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.